Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

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. 15/22

(Certificate No.)

Prodotto: **IBM RACF for z/OS Version 2 Release 4**
(Product)

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

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

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

EAL5+
(ALC_FLR.3)

Il Direttore Generale dell'ACN
(Roberto Baldoni)

Roma, 22 settembre 2022

[ORIGINAL SIGNED]

Common Criteria

Fino a EAL2 *(Up to EAL2)*

This page is intentionally left blank

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

IBM RACF for z/OS Version 2 Release 4

OCSI/CERT/ATS/03/2022/RC

Version 1.0

22 September 2022

Courtesy translation

Disclaimer: This English language translation 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	22/09/2022

2 Table of contents

3 Acronyms

3.1 National scheme

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

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target Of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other acronyms

ACEE	Accessor Environment Element
AKM	Access Key Mask
APAR	Authorized Program Analysis Report
APF	Authorized Program Facility
APPC/MVS	Advanced Program-to-Program Communication / Multiple Virtual Storage

AT-TLS	Application Transparent Transport Layer Security
BCP	Base Control Program
BDT	Bulk Data Transfer
BERD	Background Environment Random Driver
BSC	Binary Synchronous Communication
CCEB	Common Criteria Evaluated Base
CPACF	Central Processor Assist for Cryptographic Function
CVE	Common Vulnerabilities and Exposure
DAC	Discretionary Access Control
DES	Data Encryption Standard
DFS	Distributed File Service
DFSMS	Data Facility Storage Management Subsystem
EIM	Enterprise Identity Mapping
FTP	File Transfer Protocol
FVT	Functional Verification Tests
HTTP	Hypertext Transfer Protocol
ICSF	Integrated Cryptographic Service Facility
ID	Identifier
IP	Internet Protocol
IPC	Inter-Process Communication
IPD	Integrated Product Development
IPL	Initial Program Load
IT	Information Technology
JCL	Job Control Language
JES	Job Entry System
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control

MVS	Multiple Virtual Storage
NJE	Network Job Entry
OS	Operating System
PC	Program Call
PR/SM	Processor Resource/System Manager
PSW	Program Status Word
PTF	Program Temporary Fix
RACF	Resource Access Control Facility
RRSF	RACF Remote Sharing Facility
RSA	Rivest, Shamir, Adleman
SAK	System Assurance Kernel
SHA	Secure Hash Algorithm
SMB	Server Message Block
SMF	System Management Facilities
SNA	Systems Network Architecture
SSH	Secure SHell
SSL	Secure Sockets Layer
SVC	Supervisor Call
SVT	System Verification Tests
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol
TDES	Triple DES
TLS	Transport Layer Security
TSO	Time Sharing Option
TSO/E	TSO Extensions
UID	User Identifier
USS	UNIX System Services

XBM	Execution Batch Monitor
z/OS	Zero downtime Operating System

4 References

4.1 Normative references and national scheme documents

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

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

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

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

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

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

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

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

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – 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

[ETRv1] Final Evaluation Technical Report "IBM Resource Access Control Facility for z/OS V2R4", Version 1, atsec information security GmbH, 27 June 2022

[ETRv2] Final Evaluation Technical Report "IBM Resource Access Control Facility for z/OS V2R4", Version 2, atsec information security GmbH, 24 August 2022

[MLSGUIDE] "z/OS 2.4 - Planning for Multilevel Security and the Common Criteria", GA32-0891-40, 23 May 2021

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

[RACF.SAG] "z/OS Version 2 Release 4 - Security Server RACF Security Administrator's Guide", Version SA23-2289-40, 22 July 2020

[RACF.UG] "z/OS Version 2 Release 4 - Version 2 Release 4 - Security Server RACF General User's Guide", Version SA23-2298-40, 10 July 2020

[RACF-CR] Certification Report "IBM RACF for z/OS Version 2 Release 3", OCSI/CERT/ATS/09/2018/RC, Version 1.0, 16 September 2019

[RACF.SYS] "z/OS Version 2 Release 4 - Security Server RACF System Programmer's Guide", Version SA23-2287-40, 22 September 2022

[ST] "Security Target for IBM RACF for z/OS V2R4", Version 6.8a, IBM Corporation, 7 April 2022

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

[ZOS-RC] Certification Report "IBM z/OS Version 2 Release 4", OCSI/CERT/ATS/01/2018/RC, Version 1.0, 13 January 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 up to EAL2.

6 Statement of certification

The Target of Evaluation (TOE) is the product “RACF for IBM z/OS Version 2 Release 4”, developed by International Business Machines Corp. (IBM).

RACF for z/OS Version 2 Release 4 (also referred to in the following as RACF V2R4 or RACF) is the component of the z/OS operating system that is called within z/OS from any component that wants to perform user authentication, access control to protected resources and the management of user security attributes and access rights.

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

This Certification Report was issued at the conclusion of the re-certification of an earlier version of the same TOE (RACF for IBM z/OS Version 2 Release 3), already certified by OCSI (Certificate no. 7/19 of September 16, 2019 [RACF-CR]).

Due to some changes made to the product by the Developer IBM Corp., it was deemed necessary to undertake a re-certification of the TOE. Namely, a number of security functions and services of the TOE in V2R3 are no longer comprised in the scope of the TOE in V2R4, such as mandatory access control (MAC), support for security labels (Labelled Security Mode) and authentication via Kerberos. However, the Evaluators were able to reuse part of the documentation and evidences already provided in the previous evaluation.

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

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

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST], which should be read by the potential consumers of the product. 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 EAL5, 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 has been 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 RACF for z/OS Version 2 Release 4” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

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

7.2 Executive summary

TOE name	IBM RACF for z/OS Version 2 Release 4
Security Target	“Security Target for IBM RACF for z/OS V2R4”, Version 6.8a, 2022-03-07 [ST]
Evaluation Assurance Level	EAL5 augmented with ALC_FLR.3
Developer	IBM Corporation
Sponsor	IBM Corporation
LVS	atsec information security GmbH
CC version	3.1 Rev. 5
PP conformance claim	No compliance declared
Evaluation starting date	3 February 2022
Evaluation ending date	27 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 met.

7.3 Evaluated product

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

The Target of Evaluation (TOE) is IBM RACF for z/OS Version 2 Release 4 with the following elements:

- RACF for z/OS V2R4 as integral part of z/OS Version 2 Release 4 (z/OS V2.4, program number 5650-ZOS) Common Criteria Evaluated Base (CCEB) Package[1].

[1] The full list of APARs is available at item n.7 of Table 2.

RACF is the component that is called within z/OS by any component that wants to perform user authentication, access control to protected resources and the management of user security attributes and access rights (RACF stands for Resource Access Control Facility).

The TOE provides identification and authentication of users using discretionary access control, audit functionality, security management functions, program signing and verification and protection of the TSF.

The TOE security functions are described more in detail in section 7.3.2.3.

7.3.1 TOE architecture

7.3.1.1 TOE general overview

The Target of Evaluation (TOE) is the RACF component of the z/OS operating system. RACF is designed as an authentication and access manager component that manages both user security attributes and access management attributes in its own database. Users are represented within RACF by user profiles and protected resources are represented by resource profiles. Users can be members of groups where each group is represented by a group profile.

Resource profiles are structured into classes, which represent the different types of resources. Within such a class an individual profile is represented by the name of the resource, which is unique within its class. Resource manager will then query RACF whenever it needs to check a user's access rights to a resource. In this query it will specify the resource class, the name of the resource within the class, the type of access requested and the internal representation of the user that requests access. RACF is also called when a component within z/OS needs to authenticate a user. In this case the z/OS component will call RACF and will pass the identity of the user, the authentication credentials presented, the name of the component requesting user authentication and several other parameters to RACF. Based on this information RACF will authenticate the user and, if successful, create a control block representing the user with the security attributes assigned. This control block is later used when a component of z/OS calls RACF for checking access rights.

RACF also provides interfaces that allow the management of user profiles, digital certificates assigned to users, group profiles, resource profiles, access rights, security labels and general RACF attributes. RACF also provides an interface that z/OS components can call to generate a security related audit record.

Note: The RACF Remote Sharing Facility (RRSF) is not considered as a part of this evaluation and therefore must not be used in an evaluated system configuration.

7.3.1.2 Intended method of use

RACF is designed to be used by z/OS components to perform user authentication, validate a user's access to a resource, audit security critical events, manage RACF profiles and access rights to resources and RACF security parameter. It also provides interfaces to extract RACF status information. This interface is a programming interface implemented by the RACROUTE macro. RACF will check if the calling application has the right to use the function that is called. In addition, RACF exports a command interface that can be used by appropriately authorized users directly to perform management operations.

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 of users,
- Discretionary Access Control,
- Auditing,
- Security Management,
- Program Signing and Verification,
- TSF Protection.

These primary security features are supported by the domain separation and reference mediation properties of the other parts of the z/OS operating system, which ensure that the RACF functions are invoked when required and cannot be bypassed. RACF itself is protected by the architecture of the z/OS operating system from unauthorized tampering with the RACF functions and the RACF database.

7.3.2.2 Operational environment security objectives

The assumptions for the correct operation of the TOE defined in the Security Target [ST] and some aspects of Threats and Organisational Security Policies are not covered by the TOE. These aspects lead to specific security objectives to be fulfilled by the TOE operational environment. Namely, the following objectives for the operational environment have to be assured:

- Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
- Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner.
- Those responsible for the TOE must establish and implement procedures to ensure that the components that comprise the TOE are distributed, installed and configured in a secure manner supporting the security mechanisms provided by the TOE.
- Authorized users of the TOE must ensure that the comprehensive diagnostics facilities provided by the product are invoked at every scheduled preventative maintenance period.
- Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives.

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

- The z/OS operating system provides the mechanisms to separate the address spaces of RACF from any untrusted address spaces and provides the mechanisms to protect RACF programs and data within an address space from any uncontrolled access by untrusted entities.

- Those responsible for the operating system the TOE is integrated in must ensure that only programs that are fully trusted are installed.

For a complete description of the security objectives for the TOE operational environment, please refer to section 4.2 of the RACF V2R4 Security Target [ST].

7.3.2.3 Security functions

The TOE security functionality is described in detail in section 7 of the Security Target [ST]. The most significant aspects are summarized in the following:

- **Identification and Authentication**: RACF provides support for the identification and authentication of users by the means of

  - an alphanumeric RACF user ID and a system-encrypted password or password phrase.

  - an alphanumeric RACF user ID and a PassTicket, which is a cryptographically-generated password substitute encompassing the user ID, the requested application name, and the current date/time.

  - an x.509v3 digital certificate presented to a server application in the TOE environment that uses System SSL or TCP/IP Application Transparent TLS (AT-TLS) to provide TLS or SSLv3-based client authentication, and then “mapped” (using TOE functions) by that server application or by AT-TLS to a RACF user ID.

  The TOE security functions authenticate the claimed identity of the user by verifying the password/phrase (or other mechanism, as listed above) and returning the result to the trusted program that used the RACF functions for user identification and authentication. It is up to the trusted program to determine what to do when the user identification and authentication process fails. When a user is successfully identified and authenticated RACF creates control blocks containing the user’s security attributes as managed by RACF. Those control blocks are used later when a resource manager calls RACF to determine the user’s right to access resources or when the user calls RACF functions that require the user to hold specific RACF managed privileges.

- **Discretionary Access Control**: RACF implements the functions allowing resource managers within z/OS to control access to the resources they want to protect. Resources protected by RACF fall into two categories, based on the mechanisms used within RACF to describe them: Standard (e.g., MVS data sets, or general resources in classes defined by RACF or the system administrator), and UNIX (e.g., UNIX files, directories, and IPC objects instantiated by a UNIX file system). DAC rules allow resource managers to differentiate access of users to resources based on different access types.

- **Auditing**: RACF provides an auditing capability that allows generating audit records for security-critical events. RACF provides a number of logging and reporting functions that allow resource owners and auditors to identify users who attempt to access resources. Audit records are generated by RACF and submitted to another component of z/OS (System Management Facilities (SMF)), which collects them into an audit trail.
  RACF always generates audit records for such events as unauthorized attempts to access the system or changes to the status of the RACF database. The security administrator, auditors, and other users with appropriate authorization can configure which additional optional security events are to be logged. In addition to writing records to the audit trail, messages can be sent to the security console to immediately alert operators of detected policy violations. RACF provides SMF records for all RACF-protected resources (either "traditional" or z/OS UNIX-based).
  For reporting, auditors can unload all or selected parts of the SMF data for further analysis in a human-readable formats and can then upload the data to a query or reporting package, such as DFSORT™ if desired.

- **Security Management**: RACF provides a set of commands and options to adequately manage the security functions of the TOE. Additionally, RACF provides the capability of managing users, groups of users, general resource profiles, and RACF SETROPTS options.

  RACF recognizes several authorities that are able to perform the different management tasks related to the security of the TOE:

  - General security options are managed by security administrators.
  - Management of users and their security attributes is performed by security administrators. Management of groups (and to some extent users) can be delegated to group security administrators.
  - Users can change their own passwords or password phrases, their default groups, and their user names (but not their user IDs).
  - Auditors manage the parameters of the audit system (a list of audited events, for example) and can analyse the audit trail.
  - Security administrators can define what audit records are captured by the system.
  - Discretionary access rights to protected resources are managed by the owners of the applicable profiles (or UNIX objects) or by security administrators.

- **Program Signing and Verification**: RACF provides the services to support the signing and signature verification of z/OS program objects. The function can be used for both signing a program object and verifying the signature of a program object. The function is intended to be used by the z/OS program binder (for signing program objects) and the z/OS loader (to verify the signature of a program object). The signature will be generated using SHA256 as the hash function and RSA as the public key encryption algorithm. The maximum RSA key size is 4096 bit.

- **TSF Protection**: TSF protection is based on several protection mechanisms that are provided by the underlying abstract machine and z/OS operating system:
  - Privileged processor instructions are only available to programs running in the supervisor state of the processor.
  - Semi-privileged instructions are only available to programs running in an execution environment that is established and authorized by the TSF.
  - While in operation, all address spaces, as well as the data and tasks contained therein, are protected by the memory protection mechanisms of the underlying abstract machine.
  - z/OS protects the RACF address space and RACF functions from unauthorized access and either z/OS or RACF itself ensures that a caller of RACF services has the hardware or z/OS privileges (e. g. supervisor state, PSW key, APF authorization) required to invoke the service.

  z/OS address space management ensures that programs running in problem state cannot access protected memory or resources that belong to other address spaces. Access to system services – through supervisor call (SVC) or program call (PC) instructions, for example – is controlled by z/OS, which requires that subjects who want to perform security-relevant tasks be authorized appropriately.
  The hardware and firmware components that provide the abstract machine for the TOE are required to be physically protected from unauthorized access.
  Tools are provided in the TOE environment to allow authorized administrators to check the correct operation of the underlying abstract machine.
  In addition to the protection mechanism of the underlying abstract machine, z/OS also uses software mechanisms like the authorized program facility (APF) or specific privileges for programs in the UNIX system services environment to protect the TSF.

7.4 Documentation

The guidance documentation specified in Annex A - Guidelines for secure usage of the TOE is delivered to the user 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].

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

7.5 Protection Profile conformance claims

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

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3]. Namely, the requirements of EAL5 augmented by ALC_FLR.3 have been met.

All Security Functional Requirements (SFRs) have been selected or derived by extension from CC Part 2 [CC2]. In particular, the following extended components are included:

- **FIA_USB.2 Enhanced user-subject binding**: FIA_USB.2 is analogue to FIA_USB.1 except that it adds the possibility to specify rules whereby subject security attributes are also derived from TSF data other than user security attributes. FIA_USB.2 has been taken from the "Operating System Protection Profile" ([OSPP]).

- **FAU_GEN_SUB.1 Subset audit data generation**: This extended component defines a subset of the component FAU_GEN.1 as defined in part 2 of the CC. This extended component needed to be defined since RACF uses the audit trail interfaces provided by the SMF component of z/OS for trusted components that want to store their audit records in the common audit trail provided by z/OS.

For a detailed description of the extended components properties, consult section 5 of the Security Target [ST].

Users should 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 it constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

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

The evaluation was completed on 26 June 2022 with the issuance by LVS of the Evaluation Technical Report [ETRv1] which was approved by the Certification Body on 27 June 2022. An additional ETR ([ETRv2]) was delivered on 24 August 2022 including minor editorial changes. Then, the Certification Body issued this Certification Report.

7.8 General considerations on the validity of the certification

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

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

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report ([ETRv1]), issued by the LVS atsec information security GmbH, and the documents required for the certification, and considering the evaluation activities which was carried out, the Certification Body (OCSI) concluded that TOE “RACF for IBM z/OS Version 2 Release 4” meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL5, 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 EAL5, 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 semi-formal functional specification with additional error information	ADV_FSP.5	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Well-structured internals	ADV_INT.2	Pass
Semiformal modular design	ADV_TDS.4	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
Development tools CM coverage	ALC_CMS.5	Pass
Delivery procedures	ALC_DEL.1	Pass

Assurance classes and components		**Verdict**
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
Compliance with implementation standards	ALC_TAT.2	Pass
Systematic flaw remediation	*ALC_FLR.3*	Pass
Tests	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: modular design	ATE_DPT.3	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing – sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Methodical vulnerability analysis	AVA_VAN.4	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 “RACF for IBM z/OS Version 2 Release 4” are suggested to properly understand the specific purpose of the certification reading this Certification Report together with the Security Target [ST].

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

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

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

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

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

9 Annex A - Guidelines for secure usage of the TOE

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

9.1 TOE delivery

The TOE is software only and is accompanied by guidance documentation. The TOE is an integral part of the z/OS operating system and can only be obtained as part of the z/OS Version 2 Release 4 Common Criteria Evaluated Base Package.

Table 2 contains the items that comprise the different elements of the z/OS, including software and guidance. Some items not relevant to RACF have been omitted.

No	Type	Identifier	Release	Form of delivery
z/OS Version 2 Release 4 (z/OS V2.4, program number[2] 5650-ZOS) Common Criteria Evaluated Base Package				
1	SW	z/OS V2.4 Common Criteria Evaluated Base (IBM program number 5650-ZOS)	V2R4	Tape
2	DOC	z/OS V2.4 Program Directory	GI11-9848-03	Hardcopy
3	DOC	z/OS V2R4 Library V2R4 Archive file name: zOSV2R4Library.zip	V2R4	Electronic
		Download from: https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R4Library "Download all z/OS V2R4 Library publications to ZIP file"		
4	DOC	ServerPac: IYO (Installing Your Order)	n/a	Hardcopy
5	DOC	Memo to Customers of z/OS V2.4 Common Criteria Evaluated Base	n/a	Hardcopy
6	DOC	z/OS V2.4 Planning for Multilevel Security and the Common Criteria File name: e0ze100_v2r4.pdf Last updated: 2021-05-23 SHA256 checksum: 65cd99fb8f96d18ea6b2f2a7e7d2a4dae6b4c8c39cf615908cda4d1bf9f8c3ba	GA32-0891-40	Electronic
Additional Media				
7	SW	PTFs for the following APARs (required): • OA57641 (PTF UJ02099) • OA57934 (PTF UJ00393) • OA58067 (PTF UJ02223) • OA58074 (PTF UJ02931) • OA58282 (PTF UJ01931) • OA58313 (PTF UJ02442) • OA58349 (PTF UJ02614) • OA58505 (PTF UJ01875) • OA58588 (PTF UJ01732) • OA58595 (PTF UJ01957) • OA58781 (PTF UJ01929 & PTF UJ01933)	n/a	Electronic

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

No	Type	Identifier	Release	Form of delivery
		• OA58990 (PTF UJ02368 & PTF UJ02370) • OA59021 (PTF UJ02052) • OA59040 (PTF UJ02630) • OA59074 (PTF UJ02508 & PTF UJ02509) • OA59156 (PTF UJ02505) • OA59268 (PTF UJ02741 & PTF UJ02741) • PH14146 (PTF UI68531) • PH14509 (PTF UI66980) • PH14511 (PTF UI67180) These PTFs are to be obtained electronically from ShopzSeries (https://www.ibm.com/software/shopzseries)		

Table 2 - TOE Deliverables

The evaluated version of z/OS containing the TOE can be ordered via an IBM sales representative or via the ShopzSeries web application (http://www.ibm.com/software/shopzseries). When filing an order via (secured) internet services, IBM requires customers to have an account with a login name and password. Registration for such an account in turn requires a valid customer ID from IBM.

The delivery of the tapes and documentation occurs in one package, which is manufactured specifically for this customer and shipped via courier services. Additional maintenance software then needs to be downloaded by the customer via the ShopzSeries web site, following the instructions delivered with the package.

The download of the TOE guidance (see item n.3 in Table 2) is described in [MLSGUIDE], i.e. the customer downloads a guidance package from an IBM FTP Server and then verifies the package against the hash sums provided in [MLSGUIDE] or this report.

9.2 Identification of the TOE

The media and documents delivered to the customer are labelled with the product, document and version numbers as indicated in Table 2 and can be checked by the users installing the system.

The TOE reference can be verified by the administrator during initial program load (IPL) of z/OS containing the TOE, when the system identification is displayed on the system console. The operator can also issue the operator command D IPLINFO to display the z/OS version. The string "z/OS 02.03.00" should be displayed among other information.

9.3 Installation, initialization and secure usage of the TOE

The TOE is an integral part of the z/OS operating system and can only be installed as part of the evaluated configuration of z/OS.

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.

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/OS Version 2 Release 4 - Planning for Multilevel Security and the Common Criteria [MLSGUIDE],
- z/OS Version 2 Release 4 - Security Server RACF Security Administrator's Guide [RACF.SAG],
- z/OS Version 2 Release 4 - Security Server RACF General User's Guide [RACF.UG].

10 Annex B – Evaluated configuration

The following configuration of the TOE is covered by this certification.

The z/OS V2R4 Common Criteria Evaluated Base package must be installed according to the directions delivered with the media and configured according to the instructions in Chapter 7, "The evaluated configuration for the Common Criteria" of z/OS Planning for Multilevel Security and the Common Criteria [MLSGUIDE]. Also, all required PTFs as listed as item n.7 in Table 2 must be installed.

During Installation it is possible choose not to use any of the elements delivered within the ServerPac, but it is required to install, configure, and use the TOE (the RACF component) of the z/OS Security Server element.

In addition, any software outside the TOE may be added without affecting the security characteristics of the system, if it cannot run:

- in supervisor state,
- as APF-authorized,
- with keys 0 through 7,
- with UID(0),
- with authority to FACILITY resources BPX.DAEMON, BPX.SERVER, or BPX.SUPERUSER,
- with authority to UNIXPRIV resources.

This explicitly excludes:

- replacement of any element in the ServerPac providing security functions relevant to this evaluation by other third-party products;
- installing system exits that run authorized (supervisor state, system key, or APF-authorized), with the exception of the sample ICHPWX11 and its associated IRRPHREX routine;
- installing IBM Tivoli Directory Server plug-ins that have not been evaluated;
- using the Authorized Caller Table (ICHAUTAB) in RACF to allow unauthorized programs to issue RACROUTE REQUEST=VERIFY (RACINIT) or RACROUTE REQUEST=LIST (RACLIST).

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

For the RACF component of z/OS V2R4, i.e. the TOE, the following prescriptions apply:

- Do not use the RACF remote sharing facility (RRSF) in remote mode. If you use RRSF in local mode, ensure that command direction cannot be used by taking one of the following actions:
    - Ensure that the RRFSFDATA class is not active.
    - Define the profile DIRECT.* in the RRSFDATA class with UACC(NONE) and no users in the access list.
- Do not use multifactor authentication. It is possible to disable the use of multifactor authentication by making the MFADEF class inactive.

Any client that is delivered with the product that executes with the user's privileges must be used with care, since the TSF cannot protect those clients from potentially hostile programs. Passwords/phrases a user enters into those client programs that those clients use to pass to the corresponding server to authenticate the user may potentially be spoofed by hostile programs running in the user's address space. This includes client programs for telnet, TN3270, FTP, r-commands and SSH that require the user to enter his password/phrase. When using those client programs the user should take care that no untrusted potentially hostile program has been called during his session.

The following elements and element components cannot be used in an evaluated system, either because they violate the security policies stated in the Security Target [ST] or because they have been removed from the evaluated configuration due to time and resource constraints of the evaluation. As they are part of the base system, either they must be not configured for use or they must be deactivated, as described in Chapter 7 of [MLSGUIDE]:

- all Bulk Data Transfer (BDT) elements: BDT, BDT File-to-File and BDT Systems Network Architecture (SNA) NJE,
- the DFS™ Server Message Block (SMB) components of the Distributed File Service element,
- Infoprint® Server,
- JES3,
- IBM Ported Tools for z/OS HTTP Server V7.0.

In addition, the following cannot be used in the certified configuration:

- the Advanced Program-to-Program Communication / Multiple Virtual Storage (APPC/MVS) component of the BCP,
- the DFSMS Object Access Method for content management type applications,
- the RACF remote sharing facility in remote mode,

- JES2 NJE communication via TCP/IP. JES2 NJE must use SNA or BSC in the certified configuration,
- JES2 Execution Batch Monitor (XBM) facility,
- most functions of Enterprise Identity Mapping (EIM). For details, see the manual z/OS Planning for Multilevel Security and the Common Criteria ([MLSGUIDE]).

11 Annex C –Test activities

This Annex describes the effort of both the Developer and the LVS in testing activities. For the assurance level EAL5, augmented with ALC_FLR.3, such activities include the following three steps:

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

11.1 Test configuration

The Security Target requires the software packages comprising the TOE to be run on an abstract machine implementing the z/Architecture machine interface as defined in the "z/Architecture Principles of Operation" ([ZARCH]). The hardware platform implementing this abstract machine is:

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

Note that the above mentioned Crypto Express cards are not part of the TOE and therefore the implementation of the cryptographic functions provided by those cards has not been analysed.

Testing has been performed using those cards to ensure that the cryptographic functions provided by those cards work in principle. No vulnerability analysis or side channel analysis for those cryptographic functions has been performed. The claims made in the Security Target concerning the cryptographic functions therefore apply to those functions implemented in software.

The TOE may be running on those machines within a logical partition provided by a certified version of IBM PR/SM. In addition, the TOE may run on a virtual machine provided by a certified version of IBM z/VM.

IBM has tested the platforms (hardware and combinations of hardware with IBM PR/SM and/or IBM z/VM) for z/OS individually for their compliance to the z/Architecture using the Systems Assurance Kernel (SAK) suite of tests. These tests ensure that every platform provides the abstract machine interface that z/OS requires.

The test systems were running z/OS Version 2 Release 4 in the evaluated configuration. Due to the massive amount of tests, testing was performed throughout the development of the TOE. To ensure proper testing of all security relevant behaviour of the TOE, the Evaluators verified that all tests that might have been affected by any security-relevant change introduced later in the development cycle had been run on the evaluated configuration.

11.2 Functional tests performed by the Developer

RACF testing is tightly integrated into the testing of the z/OS operating system, which has been evaluated under the certification process OCSI-CERT-ATS-03-2020 ([ZOS-RC]). Therefore, the z/OS test setup and test framework also applies to RACF testing and can be summarized as follows:

- FVT (functional verification test) for z/OS is largely performed on the VICOM test system. This is an enhanced z/VM system implementing the z/Architecture abstract machine interface. It allows testers to bring up individual, virtual test machines running z/OS with access to virtualized peripherals such as disks and network connections. For the purpose of the security function tests, this environment is fully equivalent to the machines running z/OS. This environment was also used by the Evaluators for their independent testing.

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

- The test systems were running z/OS version 2 release 4 in the evaluated configuration. The technical support team provided a pre-installed system image for VICOM and for the machines running the COMSEC tests, thus ensuring that the CCEB software version was used for all tests. The additional PTFs were applied to the VICOM and COMSEC systems as they became available.

11.2.1 Testing approach

IBM's general test approach is defined in the process for Integrated Product Development (IPD) with Developer tests, functional verification tests (FVT), and system verification tests (SVT). Per release, an overall effort of more than 100 person years is spent on FVT and SVT for the z/OS components, including the RACF component. FVT and SVT is performed by independent test teams, with testers being independent from the developers. The different test teams have developed their own individual tests and test documentation tools, but all implement the requirements set forth in the IPD documentation.

For the purpose of the evaluation, FVT is of interest to the Evaluators, since the single security functions claimed in the [ST] are tested here. IBM decided to create a test bucket with the tests for the security functions, summarizing the tests in individual test plans, so that the Evaluators had a chance to deal with the otherwise overwhelming complexity of the z/OS testing.

IBM’s test strategy for the evaluation has three cornerstones:

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

- Components requiring Identification and Authentication or Access Control services call RACF. For most of these services, it is sufficient to demonstrate that these interfaces call RACF, once the testing of the RACF interface (see above) has established confidence in the correct inner workings of RACF.
- Due to the nature of the TOE and how it is embedded in z/OS, it is not possible to test it isolated. For example, a set of interfaces (the RACF callable services) is intended to be used by USS. Therefore, some USS tests contribute to the coverage and depth of testing. This also applies to components like Binder, BCP, ICSF and JES2. Those tests have been considered for the RACF testing in addition to the genuine RACF component tests.

All those additional and new test cases were determined to follow the approach of the already existing tests for the respective component.

11.2.2 Test coverage

The Developer provided a mapping between the TSF of the [ST], the TSFI in the functional specification and the tests performed. The Evaluators checked this mapping and examined the test cases to verify whether the tests covered the functions and their interfaces. Although exhaustive testing is not required, the Sponsor provided evidence that significant detail of the security functions have been tested.

The Evaluators determined that Developer tests provided the required coverage. Testing covered all TSF identified in the Security Target on all interfaces identified in the functional specification.

11.2.3 Test depth

Test depth was verified against the TOE subsystems and the security enforcing modules: For most security functions relevant to this evaluation, subsystems invoke RACF functions to take security-relevant decisions; access control, identification and authentication, security management and the generation of security-relevant audit records are mostly handled by RACF. All other security-relevant functions are implemented within the subsystems themselves, thus keeping security functions isolated within them. For the self-protection, BCP and the underlying abstract machine work together to provide memory protection and different authorization mechanisms such as APF or AKM.

The Evaluators verified that all security-relevant details of the TOE design at the level of subsystems had been taken into account for testing. In particular, testing of the RACF subsystem interfaces was performed directly at these interfaces as well as over the subsystems invoking RACF.

11.2.4 Test results

The Evaluators verified that testing was performed on configurations conformant to the Security Target ([ST]).

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

The test results provided by the Sponsor were generated on the configurations as described above. Although different test teams used different tools and test tracking databases, the Evaluators verified that all provided results showed that tests had executed successfully and yielded the expected results.

With this test environment, the Developer was able to provide proof of the necessary coverage and test depth to the Evaluators.

11.3 Functional and independent tests performed by the Evaluators

The Evaluators decided to focus on functions where the assessment of the design and Developer testing showed small gaps and potential issues with the evaluated configuration:

- Identification and authentication: The Evaluators only devised some basic testing of the identification and authentication functions for TSO/E (password, passphrase), and SSH and console timeout enforcement. A new test was extended in order to verify the usability of user names longer than 8 characters, which had been a restriction for a very long time. In addition, while focusing on user management and TSO commands, the Evaluators initially found some seemingly unexpected behaviour of non-RACF user management functions (UADS accounts), which they then further analysed and tested.

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

- Examination via test behaviour of how the presence of security labels could affect tests for standard access control.

- ACEE (Accessor Environment Elements): The Evaluators verified specific restrictions for nested ACEEs.

- Access control: The Evaluators extended the Developer tests to perform global access checking.

For the set of Developer tests to be re-run and observed, the Evaluators as overall approach chose to increase the number of different tests that have been observed over the years and focused on functionality or tests which had been changed since the previous evaluation. They also newly executed Developer tests themselves in the COMSEC test environment.

The Evaluators decided to focus on security functions claimed in the Security Target ([ST]).

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

Most Evaluator tests were run on the VICOM test system that had been set up by the Evaluators according to the specifications found in the guidance [MLSGUIDE]. Several Developer tests were rerun on the COMSEC test system. Some Developer tests included security label configurations, which are allowed in the evaluated configuration. The Evaluators have found this to be also acceptable for testing. During their testing, the Evaluators could verify that the test functions behaved as expected.

11.4 Vulnerability analysis and penetration tests

11.4.1 Testing approach

The Evaluators used the MITRE CVE portal and RACF mailing lists for finding publicly documented vulnerabilities in the TOE. In addition, they examined the ST, guidance, design, and testing information, which lead to four types of tests.

All Evaluator tests were run on the VICOM test system that had been set up by the Evaluators according to the specifications found in the guidance [MLSGUIDE] as relevant for the testing (i.e. password policies were not followed).

11.4.2 Test coverage

The Evaluators performed the following types of tests:

- fuzzing tests to test USS system calls with various invalid parameters combinations,
- simple tests using TSO-commands,
- setup of program signing support followed by low-level program modification, involving interactions between USS and MVS. While the signing and verification is done in MVS, the actual modifications in between are performed in the USS component,
- JCL scripts with potentially problematic data set concatenation statements.

Tests have been performed for the following potential vulnerable scenarios:

- insufficient parameter checking in system calls,
- data leakage through executing non-program data sets,
- missing signature verification enforcement,
- privilege elevation through data set concatenation.

11.4.3 Test depth

Basically all tests used the external interfaces of the TOE, with just the signature test accessing the external file interface through the USS component to modify data.

11.4.4 Test results

No exploitable vulnerability has been identified in the evaluated configuration.