Agenzia per la Cybersicurezza Nazionale

OCSI

Organismo di Certificazione della Sicurezza Informatica

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

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

Certificato n. *(Certificate No.)*	06/2026
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/ATS/10/2024/RC, v 1.0.
Decorrenza *(Date of 1st Issue)*	9 febbraio 2026
Nome e Versione del Prodotto *(Product Name and Version)*	IBM RACF for z/OS Version 2 Release 5
Sviluppatore *(Developer)*	IBM Corporation
Tipo di Prodotto *(Type of Product)*	Sistema Operativo
Livello di Garanzia *(Assurance Level)*	EAL5 con l’aggiunta del componente ALC_FLR.3, Conforme a CC Parte 3
Conformità a PP *(PP Conformance)*	Nessuna
Funzionalità di sicurezza *(Conformance of Functionality)*	TDS specifico per il prodotto, conforme a CC Parte 2 estesa

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

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

Roma, 9 febbraio 2026

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

[ORIGINAL SIGNED]

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

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using Common Methodology for Information Technology Security Evaluation version 3.1 release 5 for conformance to *Common Criteria for Information Technology Security Evaluation version 3.1 release 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of the National scheme for the evaluation and certification of the security in the sector of information technology (Prime Ministerial Decree of 30 October 2003 - Official Journal no. 93 of 27 April 2004) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product, by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.*

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

IBM RACF for z/OS Version 2 Release 5

OCSI/CERT/ATS/10/2024/RC

Version 1.0

9 February 2026

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	09/02/2026

2 Table of contents

3 Acronyms

3.1 National scheme

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

3.2 CC and CEM

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

3.3 Other acronyms

APAR	Authorized Program Analysis Report
APF	Authorized Program Facility

APPC/MVS	Advanced Program-to-Program Communication / Multiple Virtual Storage
ASLR	Address Space Layout Randomization
BCP	Base Control Program
BDT	Bulk Data Transfer
BERD	Background Environment Random Driver
BSC	Binary Synchronous Communication
CBPDO	Custom-Built Product Delivery Option
CM	Configuration Management
COMSEC	COMmunication SECurity
CPACF	Central Processor Assist for Cryptographic Function
CVE	Common Vulnerabilities and Exposures
DAC	Discretionary Access Control
DES	Data Encryption Standard
DFS	Distributed File Service
DFSMS	Data Facility Storage Management Subsystem
FMID	Function Modification Identifier
FTP	File Transfer Protocol
FTPS	FTP Secure
FVT	Functional Verification Testing
HTTPS	Hypertext Transfer Protocol Secure
ICSF	Integrated Cryptographic Service Facility
IPD	Integrated Product Development
IPL	Initial Program Load
IPSec	IP Security
JES	Job Entry System
LDAP	Lightweight Directory Access Protocol
NJE	Network Job Entry

OS	Operating System
PTF	Program Temporary Fix
RACF	Resource Access Control Facility
RRSF	RACF Remote Sharing Facility
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
SMB	Server Message Block
SMF	System Management Facilities
SNA	Systems Network Architecture
SREL	Subsystem Release
SSH	Secure SHell
SSL	Secure Socket Layer
SVC	Supervisor Call
SVT	System Verification Tests
TCP/IP	Transmission Control Protocol/Internet Protocol
TDES	Triple DES
TLS	Transport Layer Security
VICOM	Virtual COMputer
XBM	Execution Batch Monitor
z/OSMF	z/OS Management Facility

4 References

4.1 Normative references and national Scheme documents

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

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

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

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

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

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

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

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

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

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

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

[NIS5] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 - Condizioni per lo svolgimento di test da remoto in valutazioni Common Criteria, versione 1.1, 21 agosto 2023

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

4.2 Technical documents

[CCEBPP] Common Criteria Evaluated Base Package Plan.

[CR] IBM RACF for z/OS Version 2 Release 4 – OCSI/CERT/ATS/03/2022/RC Certification Report, 22 September 2022.

[ETRv2] Final Evaluation Technical Report RACF for IBM z/OS Version 2 Release 5, OCSI-CERT-ATS-10-2024_ETR_251114, atsec information security s.r.l., v.2.0, 14 November 2025.

[MLSGUIDE] z/OS V2.5 Planning for Multilevel Security and the Common Criteria, code GA32-0891-50, 02 August 2023, 16 January 2025.

[SIA] Security Impact Analysis: RACF 2.5, v.1.0, 16 may 2024.

[ST] Security Target for IBM RACF for z/OS 2.5 – Version 7.8 – July 15, 2025

[ZARCH] z/Architecture Principles of Operation, May 2022.

5 Recognition of the certificate

5.1 European recognition of CC certificates (SOGIS-MRA)

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

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

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

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

5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] was ratified on 8 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

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

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

This certificate is recognised under CCRA for all claimed assurance components up to EAL2 and ALC_FLR only.

6 Statement of certification

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

RACF for z/OS Version 2 Release 5 (also referred to in the following as RACF V2R5 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, NIS5]. The Scheme is operated by the Italian Certification Body "Organismo di Certificazione della Sicurezza Informatica (OCSI)", established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

This Certification Report was issued at the conclusion of the re-certification of an earlier version of the same TOE (IBM RACF for z/OS Version 2 Release 4), already certified by OCSI (Certificate no. 15/22 of September 22, 2022 [CR]).

Due to some changes made to the product by the Developer IBM Corporation, it was deemed necessary to undertake a re-certification of the TOE [SIA]. The new version of the TOE includes a new platform (z16 mainframe hardware), the updated version of the operating system (Version 2 Revision 5) new functionalities as well as existing RACF functions that where changed or enhanced after the conclusion of the RACF for z/OS Version 2 Release 4 certification process (and thus not considered in the Certificate no. 15/22).

Note that the changes have also led to the revision of the Security Target [ST]. Customers 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 "IBM RACF for z/OS Version 2 Release 5".

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

The TOE resulted compliant with the requirements of Part 3 of the CC version 3.1 Revision 5 for the assurance 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 was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product named "**IBM RACF for z/OS version 2 Release 5**" to provide assurance to the potential consumers that TOE security features comply with its security requirements.

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

7.2 Executive summary

TOE name	IBM RACF for z/OS Version 2 Release 5
Security Target	Security Target for IBM RACF for z/OS 2.5 – Version 7.8 – July 15, 2025 [ST]
Evaluation Assurance Level	EAL5, augmented by ALC_FLR.3
Developer	IBM Corporation
Sponsor	IBM Corporation
LVS	atsec information security s.r.l.
CC version	3.1 Rev. 5
PP conformance claim	No conformance claimed
Evaluation starting date	June 25, 2024
Evaluation ending date	November 17, 2025

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled and, in the configuration, shown in "Annex B – Evaluated configuration" of this Certification Report.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description refer to the Security Target [ST]. The Target of Evaluation (TOE) is IBM RACF for z/OS Version 2 Release 5 with the software components as described in Table 2, sect. 9.1.1.

IBM RACF for z/OS Version 2 Release 5 is the access control component of the operating system z/OS Version 2 Release 5 (z/OS 2.5 in the following), which is the flagship operating system for IBM z System mainframe computers. RACF is the central component within z/OS responsible for user authentication, access control, management of user security attributes, and management of access rights. RACF provides the interfaces for identification and authentication of users using different authentication mechanisms, interfaces that resource managers can use for discretionary access control to objects they define, interfaces for sophisticated security management functions, and the ability to generate audit records for security critical event.

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

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.

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.

The TOE supports its TSF database (aka RACF database) being encrypted using cryptographic mechanisms provided by the z/OS operating system.

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

The primary security features of the TOE are:

- Identification and authentication
- Discretionary access control
- Audit
- Security management
- TSF protection
- Program Signing and Verification

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.

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

7.3.2.2 Discretionary Access Control (DAC)

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).

Discretionary access control (DAC) rules allow resource managers to differentiate access of users to resources based on different access types

7.3.2.3 Auditing

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.

7.3.2.4 Security management

RACF provides a set of commands and options to adequately manage the TOE’s security functions. 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 TOE’s security:

- General security options are managed by security administrators.
- Management of users and their security attributes is performed by security administrators.
- Management of groups (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 analyze the audit trail.
- Security administrators can define the audit records that are to be registered 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.

7.3.2.5 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.

7.3.2.6 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 processor's supervisor state.
- Semi-privileged instructions are only available to programs running in an execution environment that is established and authorized by the TSF.
- While in operation, all address spaces, as well as the data and tasks contained therein, are protected by the memory protection mechanisms of the underlying abstract machine.
- 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 the secure usage of the product" is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration, and secure usage of the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in section 9 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] 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 assurance package augmented by ALC_FLR.3 have been met.

All the SFRs have been selected or derived by extension from CC Part 2 [CC2] (it includes FIA_USB.2 and FAU_GEN_SUB.1 as extended components)

It is possible to refer to the Security Target [ST] for the description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFRs) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and [NIS5] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

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

The evaluation was completed on November 17th, 2025 with the issuance by LVS of the Evaluation Technical Report v.2 [ETRv2] that has been approved by the Certification Body on 18 December 2025.

Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

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

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

The certification is not a guarantee that no vulnerabilities exist; there is a probability that exploitable vulnerabilities can be discovered after the issuance of the certificate.

This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to regularly check the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report v.2 [ETRv2] issued by the LVS atsec information security s.r.l. and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE named “IBM RACF for z/OS Version 2 Release 5” 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 EAL4 augmented with ALC_FLR.3 (augmentation in *italics* in Table 1).

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
Semiformal modular design	ADV_TDS.4	Pass
Well-structured internal	ADV_INT.2	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
Systematic flaw remediation	*ALC_FLR.3*	*Pass*
Developer defined life-cycle model	ALC_LCD.1	Pass
Compliance with implementation standards	ALC_TAT.2	Pass
Test	**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 "IBM RACF for z/OS Version 2 Release 5" are suggested to properly understand the specific purpose of the certification by reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the "*Objectives for the Operational Environment*" specified in section 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all Assumptions described in section 3.3 of the Security Target [ST] shall be satisfied.

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

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

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

9.1 TOE delivery

9.1.1 Scope of TOE supply

The following Table 2 contains the item that comprise the different elements of of z/OS V2R5, including software and guidance. The TOE can only be obtained and installed as part of the evaluated configuration of z/OS V2R5.

No	Type	Identifier	Release	Form of Delivery
z/OS Version 2 Release 5 (z/OS V2.5, program number[1] 5650-ZOS) Common Criteria Evaluated Base Package				
1	SW	z/OS V2.5 Common Criteria Evaluated Base (IBM program number 5650-ZOS)	V2R5	Electronic
2	DOC	DOC z/OS V2.5 Program Directory Archive file name: e0zpdz40.pdf SHA256 hashsum of the file: 18fcd09052a6a58dd9a7adb46379f8c3e77eb257ce1c37ad66ec65ccaa9049d5	GI11-9848-04	Digital copy
		Download from https://www.ibm.com/docs/en/zos/2.5.0		
3	DOC	z/OS V2R5 PDF Library Archive file name: zOS250-Indexed-PDF-package-(Final-refresh).zip SHA256 hashsum of the file: 52cfa67733c4e0d2c507e282d7f69f56cc13c7e7a0bbfe2a9507b86d7daaf056	V2R5	Digital copy
		Download from https://www.ibm.com/docs/en/zos/2.5.0		

[1] 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.

No	Type	Identifier	Release	Form of Delivery
4	DOC	z/OS 2.5 Installation Guides (GA32-0890-50 – Z/OS 2.5 Planning for Installation) Archive file name: e0zb100_v2r5.pdf SHA256 hashsum of the file: 6376e932f19a8468e75a7043086babc5be9fd574c7cd2f24701a5a464c70ab9c (SA23-2278-50 – ServerPac Dialog Level: 30 - Using the Installation Dialog) Archive file name: gima200_v2r5.pdf SHA256 hashsum of the file: d9eded9f48c25544ae20f512be4085e5732719531c853cc99ff5c8258d643da7	GA32-0890-50, SA23-2278-50	Digital copy
		Download from https://www.ibm.com/docs/en/zos/2.5.0		
5	DOC	Memo to Customers of z/OS V2.5 Common Criteria Evaluated Base Download from: https://www.ibm.com/software/shopzseries/ShopzSeries_public.wss	n/a	Digital copy
		Download from https://www.ibm.com/software/shopzseries/ShopzSeries_public.wss		
6	DOC	[MLSGUIDE] z/OS V2.5 Planning for Multilevel Security and the Common Criteria file name: 0ze100_v2r5.pdf Last updated: 2025-06-16 SHA256 hashsum of the document: d4011ad5ff77aa3368b0812fb74d3b7a8dceaebf81633fc95144306dd9cd3efa	GA32-0891-50	Digital copy
Additional Media				
7	SW	The following APARs (required): • (Documentation APAR) OA64593 • (Documentation APAR) OA66552	n/a	Digital copy

No	Type	Identifier	Release	Form of Delivery
		- OA56911 - OA57975 - OA60095 - OA62371 - OA66005 These PTFs are to be obtained electronically from ShopzSeries (https://www.ibm.com/software/shopzseries)		

Table 2 - TOE Deliverables

9.1.2 Delivery procedure

The evaluated version of z/OS, that includes the TOE, can be ordered via an IBM sales representative or via the ShopzSeries web application (https://www.ibm.com/software/shopzseries/ShopzSeries_public.wss). When filling 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 TOE order can be delivered to the customer only on digital form (over the internet).

The TOE order can be delivered to the customer electronically (over the internet). Order content is staged to an IBM download server and Shopz (IBM Shopz) generates a customized download page for each order. The download page includes links for order content and instructions. A typical z/OS-only ServerPac order is approximately 20 GB (compressed) in size. A typical subsystem ServerPac order is approximately 2 GB (compressed) in size.

Subsection "*Choosing the Internet download method: Direct or intermediate*" explains that with the Internet delivery option the customer also has to choose whether to download the order directly to z/OS (recommended) or download it to an intermediate node (a workstation) and then forward it to the z/OS system:

- If downloading directly to z/OS, integrity of Internet order is ensured by SHA-1 hashing algorithm and verification, if the digital signature is not verified. CBPDO (Custom-Built Product Delivery Option) and z/OSMF (z/OS Management Facility) ServerPac order packages are signed by IBM and the digital signature can be optionally verified;
- If downloading to a workstation as an intermediate node, RSA encryption is used to create a digital signature. A unique client and server public/private key pair is created. CBPDO and z/OSMF ServerPac order packages are signed by IBM and the digital signature can be optionally verified.

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

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

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

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

- If the customer is planning to download directly to z/OS, he must be familiar with the security and networking information that is required to navigate his enterprise's firewall or proxy server from z/OS (for a ServerPac or for CBPDO). Server information defines the IBM download server where the order resides. The server information specifies the IP address or hostname of the IBM download server, and the User ID and password information to access the IBM download server.
- If the customer is downloading the order to a workstation and he plans to use SMP/E RECEIVE FROMNETWORK to transfer the order to z/OS, he must update the server information to reflect the workstation's FTP server information.

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

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

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

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

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

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

9.2 Identification of the TOE by the user

The TOE is defined as follows:

- IBM RACF for z/OS 2.5 (RACF) Common Criteria Evaluated Base Package:
    - IBM z/OS Version 2 Release 5 (z/OS V2R5, program number 5650-ZOS).

- The necessary list of APARs, which has already been listed in sect. 9.1.1.

The complete set of **Function Modification Identifier FMID** is listed in [CCEBPP]

During the **Initial Program Load** (IPL) phase, the Evaluators determined that the version of the TOE is displayed on the system console as "**RELEASE z/OS 02.05.00 LICENSE = z/OS**". The same reference can be verified by the administrator when the system identification is shown on the console, and the operator can also issue the command **D IPLINFO** to display the z/OS version, with the string "**z/OS 02.05.00**" appearing among other information.

The list of installed elements with their version number can be obtained by the **SMP/E** utility, which manages and tracks the installation of software on a z/OS system, i.e., loading of elements and updating elements with fixes. The **SMP/E LIST** command allows an installation to list all versions numbers of all installed software elements and a list of all updates that have been applied to those components.

With the definition of the "*Common Criteria Evaluated Base*", IBM has set up a special ordering process for the evaluated version of the TOE. As [CCEBPP] shows (e.g., in the memo for the customers), this version is uniquely labeled as the “**CCEB version**” when customers receive the installation media.

9.3 Installation, configuration and secure usage of the TOE

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

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

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

RACF, which is included in the z/OS V2R5 Common Criteria Evaluated Base package must be installed according to the directions delivered with the media and configured according to the instructions in [MLSGUIDE] chapter 7. Also, all required APARS as listed in Table 2 above must be installed.

The installation can exclude any of the elements delivered within the ServerPac, however, **user must install, configure, and use at least the RACF component of the Security Server** (available as optional feature) and the ICSF component of Cryptographic Services.

The IEASYSxx parmlib OSPROTECT parameter specifies the operating system mitigation mode for unauthorized programs and users. OSPROTECT must be set to 1 or its equivalent value SYSTEM, which is the default.

The system must be configured with address space layout randomization (ASLR) enabled for storage access. This setting is enabled through the following DIAGxx statement: ASLR(YES).

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 from 0 through 7;

- with UID(0) or with authority to FACILITY resources BPX.DAEMON, BPX.SERVER, or BPX.SUPERUSER, or 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.
- Installation of system exits that run authorized (supervisor state, APF-authorized, or with key 0 through 7), with the exception of default installation exits that are shipped with MVS that do not compromise security:
  - Allocated/Offline Device Installation Exit.
  - Specific Waits Installation Exit.
  - Volume ENQ Installation Exit.
  - Volume Mount Exit.
  - ASREXIT—SYMREC Authorization Exit.
  - IEALIMIT—Limiting User Region Size.
  - IEAVTSEL—Post Dump Exit Name List.
  - IEFDOIXT—Edit/Check A Caller's Text Units.
  - ISGGREX0—Scanning the ENQ/DEQ/RESERVE Resource Name Lists.

  With the exception of installation exits that are shipped with RACF that do not compromise security:

  - The sample new password phrase exit, ICHPWX11 (from SYS1.SAMPLIB(RACEXITS)).
  - The REXX exec IRRPHREX (from SYS1.SAMPLIB(IRRPHREX)), which is invoked by ICHPWX11.
- Adding user own local checks to the Health Checker for z/OS because those checks run authorized. If there is the need to add user own checks, add them as unauthorized remote checks.
- Using the Authorized Caller Table (ICHAUTAB) in RACF to allow unauthorized programs to issue RACROUTE REQUEST=VERIFY (RACINIT) or RACROUTE REQUEST=LIST (RACLIST).

For the RACF component of z/OS V2R5, i.e. the TOE, the following applies:

- Global access entries should be made only for resources whose profiles specify a security label of SYSLOW. In addition, the global entry should specify an access level of READ, so that attempts to update the resource will require appropriate authorization using a profile.
- Do not create a profile in the FACILITY class protecting the resource IEC.TAPERING. If the FACILITY class is active and the profile exists, a programmer with read authorization could potentially write on a tape.
- 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. You can disable the use of multifactor authentication by making the MFADEF class inactive.

Any client that is delivered with the product that executes with the user's privileges must be used with care, since the TSF 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 the evaluated configuration, either because they violate the security policies stated in this Security Target or because they have been removed from the evaluated configuration due to time and resource constraints of the evaluation. As they are part of the base system, either they **must be not configured for use or they must be deactivated**, as described in Chapter 7, "*The evaluated configuration for the Common Criteria*" in z/OS Planning for Multilevel Security and the Common Criteria [MLSGUIDE]:

- Apache Server;
- BCPii;
- All Bulk Data Transfer (BDT) elements: BDT (FMID HBD6602), BDT File-to-File (FMID JBD6201), and BDT Systems Network Architecture (SNA) NJE (FMID JBD6202);
- the DFS Server Message Block (SMB) from the element zFS File System;
- Infoprint Server (FMIDs HMOS705, HNET7C0, HOPI7B0);
- JES3 (FMID HJS77B0);
- Kerberos;
- LDAP;
- NFS;
- PKI Services;
- SUDO;

In addition, the following cannot be used in the certified configuration (they **must be not configured for use or they must be deactivated)**:

- The Advanced Program-to-Program Communication / Multiple Virtual Storage (APPC/MVS) component of the BCP.
- The DFSMS Object Access Method for content management type applications.
- The RACF Remote Sharing Facility in remote mode.
- The multi-level security environment.
- JES2 NJE communication via TCP/IP. JES2 NJE must use SNA or BSC in the certified configuration.
- JES2 Execution Batch Monitor (XBM) facility.

The [MLSGUIDE] in section "*Software restrictions in the certified configuration*" of chapter 7 states that in the certified configuration, applications that are written in a language for which the compiler supports boundary checking, such as a stack protection mechanism, must enable boundary checking.

10 Annex B – Evaluated configuration

The Target of Evaluation is “IBM RACF for z/OS Version 2 Release 5”, developed by IBM Corporation. The TOE is software only and is accompanied by guidance documentation. The items listed in Table 2 represent the TOE.

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

10.1 TOE operational environment

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

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

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

11 Annex C – Test activity

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

11.1 Test configuration

The test systems were running IBM RACF for z/OS Version 2 Release 5 in the evaluated 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 platforms implementing this abstract machine are:

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

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. Tests have been performed using the z/VM environment.

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

11.2 Functional tests performed by the Developer

RACF testing is tightly integrated into the testing of the z/OS operating system, which has been evaluated and certified with certificate nr. 07/2025. Therefore, the z/OS test setup and test framework also applies to RACF testing and can be summarized as follows.

11.2.1 Test approach

FVT 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.

IBM has provided a common test framework for tests that can be automated. The BERD (Background Environment Random Driver) test driver submits the testcases as JES 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. Most test teams ran their manual tests in the so-called “Communication Security” (COMSEC) test environment, which provides a complete test environment in the evaluated configuration of the TOE in the different modes of operation.

The Developer provided a pre-installed system image for VICOM and for the machines running the COMSEC tests. The additional PTFs were applied to the VICOM and COMSEC systems as they became available.

IBM’s general test approach is defined in the process for Integrated Product Development (IPD) with Developer tests, FVT, and System Verification Tests (SVT). FVT and SVT test is performed by test teams, with testers being independent from the Developer. The different test teams have developed their own individual test 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 had three cornerstones:

- The major internal security interface was 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 design of z/OS, a large number of internal interfaces is also visible externally, although the interfaces are not intended to be called by external, unprivileged subjects. For these interfaces, which are basically authorized programs, operator commands, certain callable services, SVC and PC routines, testing established only that these interfaces cannot be called by unauthorized callers.

Apart from these tests, all components providing external interfaces for security functions were tested intensively. For the current version of RACF for z/OS this included additional tests for enhancements of the already existing TOE components. All new test cases were determined to follow the approach of the already existing tests for the respective component.

For components providing cryptographic functions, testing was performed with and without hardware cryptographic support in order to test the correct usage of the hardware cryptographic functions, if present, and the correct implementation of the software implementation within the TOE.

11.2.2 Test Coverage

The Evaluators verified the complete coverage between the test cases in the test documentation provided by Developer and the TSFIs described in the functional specification. The Evaluators verified that the test cases are sufficient to demonstrate the internal behaviour and properties of the TSF.

11.2.3 Test results

The actual test results of all Developer’s tests were consistent with the expected ones.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Test approach

The Evaluators performed tests following the CEM approach to test every security function, without striving for exhaustive testing: Evaluators devised a test strategy for the tests they intended to re-run from the developer's tests and the set of tests they were developing themselves.

The Evaluators performed testing remotely by connecting to the test environment using IBM hardened laptops as specified. The Developer set up the test environment with the actual TOE model in Poughkeepsie, New York, USA. The testing was performed in July 2025.

11.3.2 Test result

The Evaluators involved in the tests decided to focus the sampling based on [ST] functional claims related to TOE security functions. A claim does not necessarily cover new functionality, whether they are introduced in previous versions of the TOE but were just re-worded in the current [ST] and thus were assigned new claim identifiers, these were classified as *minor.*

Changes that were new in RACF for z/OS Version 2 Release 5 are classified as *major*. With this concept in mind, the sampling of the Evaluators is based on the re-execution of the tests associated with a major claim or one that has undergone an update since the previous evaluation (*minor*).

Finally, the Evaluators considers the strategy used to be reasonable also because the security functions of the "core" system had already been investigated several times, and no indication had been found throughout the evaluation that any changes in the system behaviour could be expected for the unchanged security functionality.

The Evaluators chose to observe the developer tests while they performed a sample of their test cases. This setup was preferred to setting up an own instance of COMSEC, which would have required the transfer of all instrumentation software to that system. Rather, the Evaluators decided to observe test runs from the different test teams, which would also allow them to interview the testers and understand their tests and methodology in a more efficient manner than from the investigation of the test documentation alone. Therefore, the Evaluators scheduled a series of test sessions with the different test teams.

The sampled developer's tests were run successfully, and the Evaluators verified the correct behaviour of the TSFIs and TSFs and the correspondence between expected results and achieved results for each test. All test cases devised by the Evaluators were run successfully and all the test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked on the test environment and TOE already used for the functional test activities, verifying that the TOE and the test environment were properly configured. The Evaluators analysed the Security Target [ST], design documentation, and test results for potential vulnerabilities. In addition, the Evaluators performed a search on public sources for known or claimed potential vulnerabilities of the TOE or components of the TOE. After an analysis of different potential vulnerabilities, the Evaluators devise the following four penetration tests:

- Disclosure of data.
- Modification of a signed program.
- Attempt to perform a privilege escalation.
- Fuzzing through USS system calls to RACF callable services.

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