Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

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

Certificato n. 7/19

(Certification No.)

Prodotto: IBM RACF for z/OS Version 2 Release 3

(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 Dirigente
(Dott. Antonello Cocco)

Roma, 16 settembre 2019

Common Criteria

Fino a EAL2 *(Up to EAL2)*

This page is intentionally left blank

Organismo di Certificazione della Sicurezza Informatica

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

IBM RACF for z/OS Version 2 Release 3

OCSI/CERT/ATS/09/2018/RC

Version 1.0

16 September 2019

Courtesy translation

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

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	16/09/2019

2 Table of contents

3 Acronyms

ABEND Abnormal End

ACL Access Control List

AKM Authorized Key Mask

APAR Authorized Program Analysis Report

APF Authorized Program Facility

BCP Base Control Program

BDT Bulk Data Transfer

CC Common Criteria

CCEB Common Criteria Evaluated Base

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

CPACF Central Processor Assist for Cryptographic Functions

DAC Discretionary Access Control

DFS Distributed File Service

DFSMS Data Facility Storage Management Subsystem

DPCM Decreto del Presidente del Consiglio dei Ministri

EAL Evaluation Assurance Level

FTP File Transfer Protocol

FVT Functional Verification Test

HTTP HyperText Transfer Protocol

ICSF Integrated Cryptographic Service Facility

ID Identifier

IPC Inter-Process Communication

IPD Integrated Product Development

IPL Initial Program Load

IT	Information Technology
ITDS	IBM Tivoli Directory Server
JES	Job Entry Subsystem
LDAP	Lightweight Directory Access Protocol
LDBM	LDAP Data Base Manager
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
MAC	Mandatory Access Control
NIS	Nota Informativa dello Schema
NJE	Network Job Entry
OCSI	Organismo di Certificazione della Sicurezza Informatica
PC	Program Call
PKI	Public Key Infrastructure
PP	Protection Profile
POSIX	Portable Operating System Interface for Unix
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
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMB	Server Message Block
SMF	System Management Facilities
SSH	Secure Shell
SSL	Secure Sockets Layer

ST	Security Target
SVC	Supervisor Call
SVT	System Verification Tests
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSO/E	Time Sharing Option/Extensions
UID	User ID
USS	UNIX System Services

4 References

4.1 Criteria and regulations

[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

[ETR] Final Evaluation Technical Report “IBM Resource Access Control Facility for z/OS V2R3”, OCSI-CERT-ATS-09-2018_ETR_190628_v1, Version 1, atsec information security GmbH, 28 June 2019

[MLSGUIDE] “z/OS Version 2 Release 3 - Planning for Multilevel Security and the Common Criteria”, Version GA32-0891-30, 15 May 2019

[RACF.SAG] “z/OS Version 2 Release 3 - Security Server RACF Security Administrator's Guide”, Version SA23-2289-30, July 2017

[RACF.UG] “z/OS Version 2 Release 3 - Security Server RACF General User's Guide”, Version SA23-2298-30, July 17, 2017

[ST] Security Target for IBM RACF for z/OS V2R3, Version 5.5, IBM Corporation, 26 June 2019

[ZARCH] “z/Architecture Principles of Operation”, Version SA22-7832-11, September 2017

[ZOS-RC] Certification Report “IBM z/OS Version 2 Release 3”, OCSI/CERT/ATS/01/2018/RC, Version 1.03, 1 July 2019

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]) was ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

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

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

This certificate is recognised under CCRA up to EAL2.

6 Statement of Certification

The Target of Evaluation (TOE) is the product “IBM RACF for z/OS Version 2 Release 3”, developed by International Business Machines Corp. (IBM).

RACF for z/OS Version 2 Release 3 (also referred to in the following as RACF V2R3 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).

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

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level 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 "IBM RACF for z/OS Version 2 Release 3" 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 3
Security Target	Security Target for IBM RACF for z/OS V2R3, Version 5.5 [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	27 November 2018
Evaluation ending date	28 June 2019

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 3 with the following elements:

- RACF for z/OS V2R3 as integral part of z/OS Version 2 Release 3 (z/OS V2.3, program number 5650-ZOS) Common Criteria Evaluated Base Package

RACF is the component 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 (RACF stands for Resource Access Control Facility).

The TOE provides identification and authentication of users using different authentication mechanisms, both discretionary and mandatory access control with support for security labels, 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 they need to check a user's access rights to a resource. In this query they 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, and manage RACF profiles, 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 called. In addition RACF exports a command interface that can be used by appropriately authorized users directly to perform management operations.

The Security Target [ST] specifies two modes of operation: a "normal" mode where labeled security features are not configured as required and a "Labeled Security Mode" where labeled security is configured as described. In "Labeled Security Mode" additional security functionality is active, which is marked with "Labeled Security Mode" in this document. Note that when functions of labeled security are configured differently than specified in the Security Target, the security functionality defined for the "normal" mode still works but additional restrictions may be imposed due to the way the functions for labeled security are configured.

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
- Mandatory Access Control and support for security labels (Labeled Security Mode)
- 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. 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 V2R3 Security Target [ST].

7.3.2.3 Security functions

The TOE security functionality is described in detail in sect.1.4.2 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.

- a Kerberos™ v5 ticket presented to a server application in the TOE environment that supports the Kerberos mechanism, and then mapped by that application through the GSS-API programming services. The TOE also provides functions that enable the application server to validate the Kerberos ticket, and thus the authentication of the principal. The application server then translates (or maps) the Kerberos principal 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 (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). DAC rules allow resource managers to differentiate access of users to resources based on different access types.

- **Mandatory access control (MAC) and support for security labels**: In addition to DAC, RACF provides MAC functions that are required for Labeled Security Mode, which impose additional access restrictions on information flow on security classification. Users and resources can have a security label specified in their profile. Security labels contain a hierarchical classification (security level), which specify the sensitivity (for example: public, internal use, or secret), and zero or more non-hierarchical security categories (for example: PROJECTA or PROJECTB).
  The access control enforced by the TOE ensures that users can only read labeled information if their security labels dominate the label of the information, and that they can only write to labeled information containers if the label of the container dominates the subject's label, thus implementing the Bell-LaPadula model of information flow control. The system can also be configured to allow write-down for certain authorized users.

- **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.
  - In Labeled Security Mode: management of MAC attributes is performed 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).
  - In Labeled Security Mode: users can choose their security labels at login, for some login methods. (Note: this also applies in normal mode if the administrator chooses to activate security label processing.)
  - 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 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 (provided by the RACF environment)**: 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 customer together with the product. The guidance documentation contains all the information for installation, configuration and secure usage of the TOE in accordance with the requirements of the Security Target [ST].

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

7.5 Protection Profile conformance claims

The Security Target [ST] 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 analog 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 28 June 2019 with the issuance by LVS of the Evaluation Technical Report [ETR], which was approved by the Certification Body on 30 July 2019. Then, the Certification Body issued this Certification Report.

7.8 General considerations on the validity of the certification

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

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

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR], issued by the LVS atsec information security GmbH, and the documents required for the certification, and considering the evaluation activities which was carried out, the Certification Body (OCSI) concluded that TOE "IBM RACF for z/OS Version 2 Release 3" 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
Identification of security measures	ALC_DVS.1	Pass

Assurance classes and components		Verdict
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 “IBM RACF for z/OS Version 2 Release 3” 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 sect. 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 realized to counter threats from unexperienced, 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 3 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 3 (z/OS V2.3, program number1 5650-ZOS)[1] Common Criteria Evaluated Base Package				
1	SW	z/OS V2.3 Common Criteria Evaluated Base (IBM program number 5650-ZOS). This package contains the TOE.	V2R3	Tape
2	DOC	z/OS V2.3 Program Directory	GI11-9848-02	Hardcopy
3	DOC	z/OS V2.3 Documentation Collection Hashsums for download (ftp:// public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/c27843007-CC_Eval.zip) **SHA224**: 84851b31fbf1bb4056944796b6f766c9d7ba1d36b4c26cf62d989c12 **SHA256**: 53d4a0ba82a3b67d031f3876fbceb88186b7d1ff2fe6af4ca6e8f7a7a422546d **SHA384**: d8d8b6c595d13ecb7a19f056395f62ea155a848c8f07a51d63ce812a7c485e73a9b83d26fee16cf67d6c452aaa794ef2 **SHA512**: 6c7207620867fc2d9ff80e72e31115a568c9606cf3b866a962739a297b32ab9206e4ead0bc2ebbb244f98c10b0cf906973b913d17d2970360fb4ff721e8ff45e		
4	DOC	ServerPac: IYO (Installing Your Order)	n/a	Hardcopy
5	DOC	Memo to Customers of z/OS V2.3 Common Criteria Evaluated Base	n/a	Hardcopy
6	DOC	z/OS V2.3 Planning for Multilevel Security and the Common Criteria; Document No. GA32-0891-30 Hashsum of the document: **SHA256**: 48cee926a44883fd7cb93b49e995b7f19f5da309b48a24aaef917a9738001b8f		
Additional Media				
14	SW	PTFs for the following APARs (required). It should be noted, that this list includes APARs that are not directly applicable to the TOE, but to the base z/OS operating system. APARs and related PTFs relevant for the TOE are marked in **bold**: • **OA52110 (PTF UA93049)** • OA52192 (PTF UA93490) • OA52722 (PTF UA93924) • OA52830 (PTF UA92871)	n/a	Electronic

[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. The string z/OS Version 2 Release 3 uniquely identifies the TOE.

No.	Type	Identifier	Release	Form of Delivery
		• **OA52834 (PTF UA94035)** • OA52932 (PTF UA93783) • OA53036 (PTF UA93779) • OA53223 (PTF UA94801) • OA53626 (PTF UA95087) • OA53643 (PTF UA94136) • OA53716 (PTF UA95334) • OA53755 (PTF UA94051) • OA53759 (PTF UA96307) • OA53764 (PTF UA94053) • OA53775 (PTF UA93986) • OA53792 (PTF UA94309) • OA53799 (PTF UA93869) • OA53809 (PTF UA94644) • OA53813 (PTF UA95903) • OA53818 (PTF UA95262) • OA53856 (PTF UA94198) • **OA53930 (PTF UA95160)** • OA53934 (PTF UA94422) • **OA53946 (PTF UA94612)** • OA53961 (PTF UA95898) • OA53962 (PTF UA95899) • OA54024 (PTF UA93979) • OA54059 (PTF UA94332) • OA55396 (PTF UA97378) • OA55435 (PTF UA96829) • OA55444 (PTF UA96532) • OA55483 (PTF UA96530) • OA55692 (PTF UA96528) • OA56409 (PTF UA97819) • OA56418 (PTF UA97888) • PH04246 (PTF UI59826) • PI82795 (PTF UI48034) • PI86170 (DOC) • PI87297 (PTF UI50688) • PI87424 (PTF UI50691) • PI87427 (PTF UI50685) • PI87482 (PTF UI53437) • PI87585 (PTF UI52347) • PI87635 (PTF UI50686) • PI87646 (PTF UI50680) • PI87652 (PTF UI50681) • PI89400 (PTF UI52529) In addition, the following APAR/PTFs needs to be obtained: **OA57638 (PTF UA99514, UA99513)**. 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 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 #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 hashsums provided in [MLSGUIDE] or this report.

9.2 Identification of the TOE

The media and documents delivered to the customer are labeled 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 3 - Planning for Multilevel Security and the Common Criteria [MLSGUIDE]
- z/OS Version 2 Release 3 - Security Server RACF Security Administrator's Guide [RACF.SAG]
- z/OS Version 2 Release 3 - 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 V2R3 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 #14 in Table 2 must be installed.

Installations may choose not to use any of the elements delivered within the ServerPac, but are 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.

RACF:

- 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, ssh, all LDAP utilities and Kerberos administration utilities 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 Developer and 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 package 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 zEnterprise zEC12/BC12 with CPACF DES/TDES Enablement Feature 3863 active, with Crypto Express3 or Crypto Express4S card, and with or without the zEnterprise BladeCenter Extension (zBX).
- IBM z13/z13s with CPACF DES/TDES Enablement Feature 3863 active, with Crypto Express4, Crypto Express4S or Crypto Express5S cards, with or without the zEnterprise BladeCenter Extension (zBX).
- IBM z14 with CPACF DES/TDES Enablement Feature 3863 active, with Crypto Express5S or Crypto Express6S cards.

Note that the above mentioned Crypto Express cards are not part of z/OS and therefore the implementation of the cryptographic functions provided by those cards has not been analyzed.

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 or by the CPACF feature.

The z/OS operating system containing the TOE may be running on those machines within a logical partition provided by a certified version of IBM PR/SM. In addition, the z/OS operating system containing 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 3 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 behavior of the TOE, the Evaluators verified that all tests that might have been affected by any security-relevant change introduced late 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 and certified under OCSI/CERT/ATS/01/2018 [ZOS-RC]. Therefore, the z/OS test setup and test framework also applies to RACF testing and can be summarized as follows:

- 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. COMSEC is an environment that can be operated in standard mode or Labeled Security mode. 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 3 in the evaluated configuration. The SDF 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, with any security-relevant tests for the PTFs being successfully re-run. For some APARs claimed by the ST, which have not been installed on the test systems, an analysis of their security impact revealed that they actually have no effect at all on the TOE functionality being tested.

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 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 Security Target [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 of z/OS, and therefore RACF, has three cornerstones:

- In z/OS testing, the major internal security interface was the interface to RACF, which is tested exhaustively by the RACF test group. This testing mostly serves for RACF as the testing of RACF's external interfaces.

- Components requiring Identification and Authentication or Access Control services call RACF (with the exception of LDAP LDBM, which implements its own access control). 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.

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, CS390, ITDS, 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.

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 Developer provided a mapping between the TSF of the Security Target [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.

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.

11.2.3 Test results

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.

The testing provided was valid for both the standard mode and the Labeled Security mode of operation, with the exception of tests for multilevel security features, which were relevant to Labeled Security mode only. The test systems configured for Labeled Security mode are compliant to standard mode as well, so that tests run on these systems were always applicable to both modes of operation. For COMSEC, all applicable tests were run in dedicated Labeled Security mode and standard mode configurations.

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. 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 independent Evaluator testing followed the [CEM] guidance to test every security function, without striving for exhaustive testing. For their own tests, the Evaluators decided to focus on the most important security functions of the TOE in order to provide independent verification of their correct operation:

- Identification and authentication: The Evaluators would only devise some basic, mostly implicit testing of the Identification and authentication functions in TSO/E, ftp, su and JES, because these functions would be exercised extensively during the test activity by the testers. The tests focused on the Kerberos based authentication mechanisms.

- Discretionary access control: The Evaluators focused on UNIX System Services ACLs, which also implicitly test UNIX permission bits. Other DAC tests involved:

    - USS IPC (all system calls for messages, semaphores and shared memory);

  - DAC for different USS objects (device special files, IPC objects, directories);
  - z/OS dataset access;
  - security-relevant USS system calls which are interfacing RACF internally.

- Mandatory Access Control: The Evaluators re-ran their own tests on mandatory access control checks for data sets and Unix System Services files as their own regression tests. Testing of the write-down override capability provided by FACILITY class profiles was also performed.
- Audit: Tests were used to check auditing of changes to the system clock.
- Security Management: The Evaluators decided to devise no special tests here, since the setup of the test environment and the setup/cleanup of the tests would already include a major portion of the TSF found here.
- TOE Self Protection: The only function to be suitably testable is object re-use, where the Evaluators decided to focus on the issue of memory pages probably containing left-over information.

For the set of Developer tests to be re-run and observed, the Evaluators chose an approach supplementing their own tests and focusing on functionality changed since the previous evaluation.

The Evaluators decided to focus on security functions claimed in the Security Target and not to run tests demonstrating that functions requiring authorization would fail when invoked unprivileged. This was in part due to the fact that the Evaluators had experienced already sufficient issues with protection of security functions while bringing up the system in its evaluated configuration, following the guidance in [MLSGUIDE].

Apart from the tests re-run by the Evaluators or during dedicated sessions set up for the Evaluators to observe the testers running those tests, the Evaluators gained confidence in the Developers' test efforts during their extended stay at the Developer site, where they discussed with testers issues of testing or interpretations of the CC requirements, and were witnessing test executions while the test bucket was being created. The Evaluators had already interviewed testers during the site visits and examined the test databases with test cases and test results and test execution records.

All 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], and on the COMSEC system set up by IBM and verified by the Evaluators to be in the evaluated configuration. One exception to this were additional patches, which the Developer recommends for the TOE, even though they were not part of the CC test installation. The Evaluators examined the information on these patches provided by the Developer and found that they do not affect the behaviour of the security functions under test.

During their testing, the Evaluators could verify that the test functions behaved as expected.

11.4 Vulnerability analysis and penetration tests

As for vulnerability assessment, the changes introduced in V2R3 with respect to the previous version of the TOE did not yield major potential for penetration testing.

The Evaluator penetration testing covered the following area, which in all previous evaluations has never been covered:

- USS Syscalls as Frontends to RACF Services.

The penetration testing examined the available system calls, supplying random arguments. No specific security function was subject to testing here. However, the system calls represent the full set of functions available to USS subjects.

Any problem that would occur during testing, would potentially subvert the security functions behind that system call. The USS subsystem, as well as RACF have been subject to testing.

Since the TOE withstood the penetration testing efforts in all tests, the Evaluators could conclude that no attack scenario with potential Moderate or lower can be completed successfully in the operating environment of the TOE as a whole. No residual vulnerabilities have been identified.