IBM® z/OS® Version 2 Release 1 Security Server RACF® Signature Verification Module version 1.0

FIPS 140-2 Non-Proprietary Security Policy

Policy Version 1.2

IBM Systems & Technology Group
System z Development
Poughkeepsie, New York

July 18th, 2016

Table of Contents

Scope of Document

This document describes the services that the IBM® z/OS® Version 2 Release 1 Security Server RACF® Signature Verification Module (“IRRPVERS” or “module”) provides to crypto officers and end users, and the policy governing access to those services. It complements official product documentation, which concentrates on application programming interface (API) level usage and environmental setup.

Module Description

The IBM® z/OS® Version 2 Release 1 Security Server RACF® Signature Verification Module in its FIPS 140-2 configuration consists of:

- CP Assist for Cryptographic Function (CPACF) to provide Secure Hash Algorithm operations

- The core software component (IRRPVERS) that is utilized when verifying signed code. It is comprised of the following set of binaries:

Binary Component
IRRPVERS
IRRRPS11
IRRRPS21
IRRRPS31
IRRRPS32
IRRRPS50
IRRRPS51
IRRRPS60
IRRRPS70
IRRRPS71
IRRRPS72
IRRRPS80
ICHSGF00
IRRRCP00
IRRPVK01
IRRBER01
IRRBER04
IRRBER05
IRRBER07
IRRJCLIC
IRRJCRTE
IRRJHASH
IRRRCOMR
IRRRCOM1
IRRERR02

Table 1: RACF Program Signature Verification Module Software Binaries

A separate software component, IRRVERLD, which is outside the logical boundary of the module loads the IRRPVERS component automatically during system boot without requiring operator intervention.

Cryptographic Module Specification

The IBM® z/OS® Version 2 Release 1 Security Server RACF® Signature Verification Module is classified as a multi-chip standalone software-hybrid module for FIPS Pub 140-2 purposes. The RACF Program Signature Verification module consists of software-based cryptographic algorithms, as well as hashing algorithms provided by the CP Assist for Cryptographic Function (CPACF).

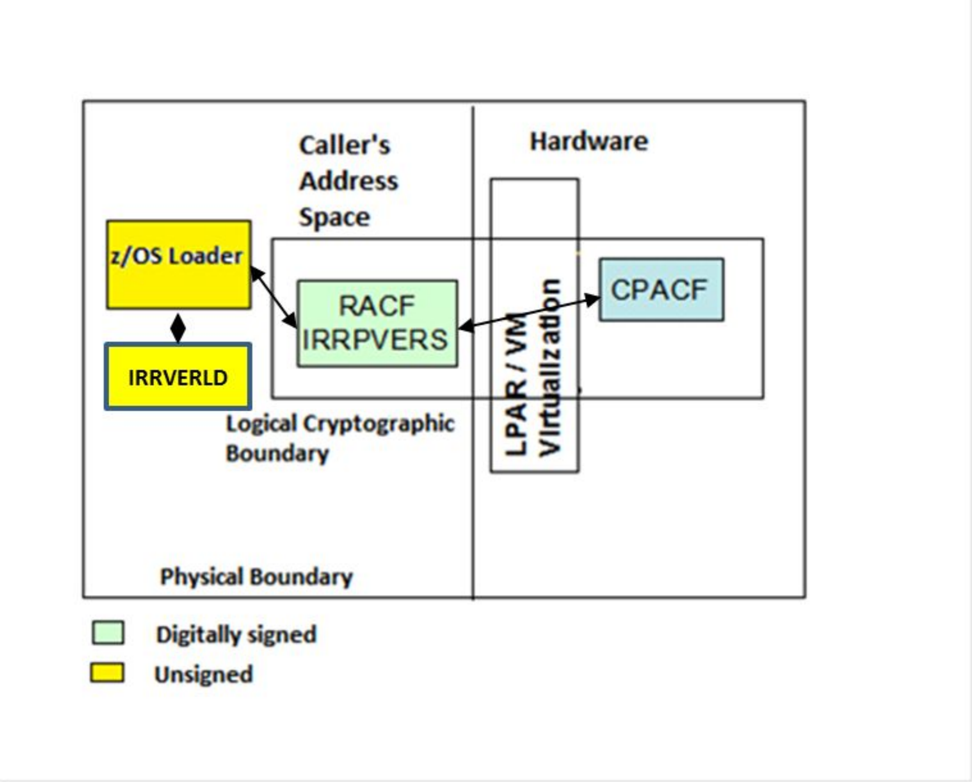

Figure 1: Physical and Cryptographic boundaries

RACF Program Signature Verification validation was performed using the z/OS Version 2 Release 1 operating system running on a IBM z13 processor with the "*CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 (Base GPC)*" enabled.

Security level

This document is the security policy for the IBM® z/OS® Version 2 Release 1 Security Server RACF® Signature Verification Module with Level 1 overall security as defined in FIPS Pub 140-2 [1].

Type / Names	Version
Software components RACF IRRPVERS	RACF level HRF7790
Hardware components CPACF	Hardware – CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 with System Driver Level 22H (FC 3863 EC N98775 Drv 22H)

Documentation	z/OS Security Server RACF Callable Services (SA23-2293-00) z/OS Security Server RACF System Programmer's Guide (SA23-2287-00) z/OS Security Server RACF Security Administrator's Guide (SA23-2289-00) z/OS Security Server RACF Command Language Reference (SA23-2292-00) z/OS Security Server RACF Messages and Codes (SA23-2291-00)

Table 2: RACF Program Signature Verification Module Components

Cryptographic Module Security Level

The module is intended to meet requirements of Security Level 1 overall, with certain categories of security requirements not applicable (Table 3: Module Security Level Specification).

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of other attacks	N/A
Overall	1

Table 3: Module Security Level Specification

Ports and Interfaces

As a multi-chip standalone module, the RACF Program Signature Verification Module physical interfaces are the boundaries of the host running RACF Program Signature Verification module code.

Data input and data output are provided in the variables passed on the callable service invocation, generally through user-supplied buffers. Hereafter, the callable services will be referred to as "API".

User-induced or internal errors do not reveal any sensitive material to callers. Documentation for the API lists the return and reason codes. A complete list of all return and reason codes returned by the APIs is specified in the *z/OS Security Server RACF Callable Services* manual.

Cryptographic bypass capability is not supported by the RACF Program Signature Verification module

Significant interconnections and data flow

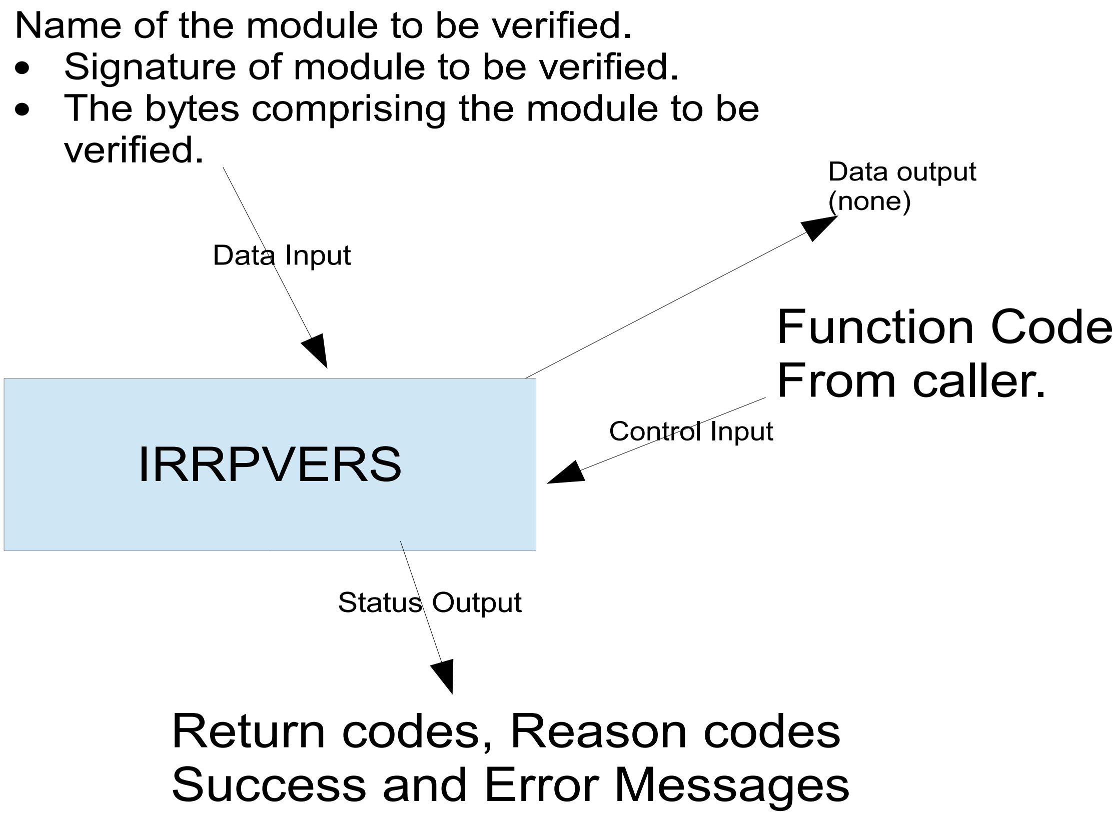
Name of the module to be verified.
• Signature of module to be verified.
• The bytes comprising the module to be verified.
Data Input
Data output (none)
Function Code From caller.
Control Input
IRRPVERS
Status Output
Return codes, Reason codes
Success and Error Messages

Figure 2: Data input, data output, control input and status output

FIPS Interface	Physical Port	Module Interface
Data input	N/A	API input parameters
Data output	N/A	N/A
Control input	N/A	Function code
Status output	N/A	API return codes, reason codes, error and success messages
Power Input	PC Power Supply Port	N/A

Table 4: Module Security Level Specification

Roles, Services and Authentication

Roles

The module supports the verification of signed programs, including the IRRPVERS verification module.

There are 2 roles, crypto officer and user. All roles are implicitly assumed based upon the service invoked.

Role	Purpose / Permitted Actions	Type of Authentication	Authentication Data	Strength of Mechanism
User	Request to verify a signed program	None	None	N/A
Crypto officer	Configure system to make the IRRPVERS module available to verify signed program on behalf of user.	Implicit[1]	N/A	N/A

Table 5: Token Role Descriptions and Authentication Mechanisms

[1] The Crypto officer role is not explicitly authenticated but assumed implicitly on implementation of the module's installation and usage sections.

Services

The module provides a program verification service. This service is requested automatically by the operating system when it detects that a signed program is being loaded into storage. FIPS Approved Algorithms are shown in Table 6 and Services in Table 7.

Algorithm	Notes	Modes	Approved If yes, Cert #
Software			
RSA Verify for module integrity (1024 and 2048 bits) (RACF R_PgmSignVer callable service)	PKCS #1 v1.5 using SHA-256 (IRRPVERS)	N/A	Cert. #1979
CPACF			
SHA-256 (KIMD and KLMD machine instructions)	FIPS 180-4	N/A	Cert. #3196

Table 6: FIPS Approved Algorithms

Service	Notes	Roles		CSPs	CSPs' access
Module Status		**Crypto Officer**	**User**		**Read (R), Write**

					(W) or Execute (EX)
Query mode	Check if module is available (message ICH448I in the system log)	Yes	Yes	N/A	N/A
Integrity Checks					
Power up tests	Automatic before first use	Yes	No	N/A	N/A
Self-tests	Requires system re-boot	Yes	No	N/A	N/A
Signature Verification					
Verify Program Signature	Verify the PKCS #1 v1.5 signature of a program to be loaded	No	Yes	N/A	N/A

Table 7: Services and associated CSPs

All service inputs and outputs are described in the *z/OS V2R1 Security Server RACF Callable Services* manual and the *z/Architecture Principles of Operation* manual. The configuration specifications for the Crypto Officer are specified in the *z/OS V2R1 Security Server RACF Security Administrators Guide*.

Operational Environment

Installation and Invocation

RACF level HRF7790 is installed as part of the z/OS Version 2 Release 1 ServerPac using the “Installing Your Order” documentation provided with the ServerPac (prepackaged tailored z/OS installation including RACF).

The RACF Signature Verification module (IRRPVERS) is shipped as part of the Security Server RACF component. IRRPVERS is the only RACF FIPS cryptographic relevant module, the rest of the RACF component is deemed as not being cryptographically relevant. Therefore is not considered part of the cryptographic boundary.

The RACF Signature Verification module is written in PL/X, with certain functionality contained within assembler, such as functions that utilize the CPACF.

The RACF Signature Verification cryptographic module is intended to operate within the z/OS Version 2, Release 1 in a single-user mode of operation.

Using RACF Signature Verification module in a FIPS 140-2 approved manner assumes that the following defined criteria are followed:

- The Operating System enforces authentication method(s) to prevent unauthorized access to Module services.

- All host system components that can contain sensitive cryptographic data (main memory, system bus, disk storage) must be located within a secure environment.

- The RACF Signature Verification module setup procedures documented in the RACF Security Administrators Guide.
- The CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 must be installed and enabled.

Approved Mode of Operation

Configuring the cryptographic module for approved mode of operations is a one-time setup. Once configured to verify the signatures of signed executable modules, no additional steps are required to ensure that IRRPVERS is executing in an approved mode of operation. Detailed setup guidance for the cryptographic module is provided in the *z/OS V2R1 Security Server RACF Security Administrators Guide* manual and summarized below:

- Create a key ring to use for signature verification
- Add the TRUST attribute to the code-signing CA certificate supplied with RACF
- Add the code-signing CA certificate to the key ring previously created
- Create a FACILITY class profile that specifies the name of the key ring previously created
- Control execution of the cryptographic module using a profile in the FACILITY class
- Correct setup can be confirmed at this point by executing the IRRVERLD program

At this point the cryptographic module is configured to run in the approved mode. The module will be automatically started each time the system is re-started Additional setup (described in the *z/OS V2R1 Security Server RACF Security Administrators Guide* manual) is required to identify executable programs that should have their signatures verified prior to being allowed to execute.

Mitigation of Other Attacks

The Mitigation of Other Attacks security section of FIPS 140-2 is not applicable to the RACF Program Signature Verification cryptographic module.

Physical Security

The RACF Program Verification Module inherits the physical characteristics of the host running it, including the physical characteristics from CPACF. The software part of the RACF Program Signature Verification has no physical security characteristics of its own. Figure 2 illustrates an IBM System z13 mainframe computer.

The CP Assist for Cryptographic Function (CPACF) (see Figure 3) offers the full complement of the Triple-DES algorithm, Advanced Encryption Standard (AES) algorithm and Secure Hash Algorithm (SHA). For this module, only the SHA-256 CPACF implementation is utilized.

CPACF Physical Design: Each set of two microprocessors (cores) on the quad-core chip share a Co-Processor Unit (CoP), which implements the crypto instructions and also provides the hardware compression function. The compression unit is integrated with the CP Assist for Cryptographic Function (CPACF), benefiting from combining (sharing) the use of buffers and interfaces. The CoP is located on the processor die and is connected to two cores and to L2 cache with dedicated buses.

Figure 3: IBM z13 Mainframe Computer

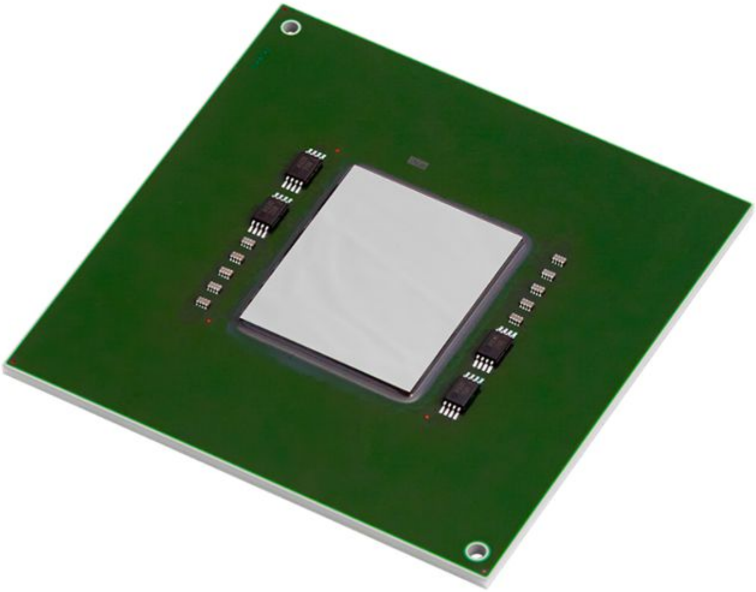

Figure 4: IBM CPACF

EMI/EMC

EMI/EMC properties of RACF Signature Verification are not meaningful for the RACF Signature Verification module itself. Systems utilizing the module's services have their overall EMI/EMC ratings determined by the host system. The validation environments meet the requirements of 47 CFR FCC PART 15, Subpart B, Class A (Business use).

Self-Tests

RACF Signature Verification Module

The RACF Signature Verification module implements self-tests to check proper functioning of the module including power-up self-tests. If a self-test fails the appropriate return and reason code along with an error message is returned as documented in the *z/OS V2R1 Security Server RACF Callable Services* manual and the *z/OS V2R1 Security Server RACF Messages and Codes* manual

Startup Self-Tests

"Power-up" self-tests consist of a software integrity test. The module integrity test is automatically performed during loading. If the test fails, the module will be returned to the uninitialized state, and a message is issued. If the message indicates a configuration issue, the user can use RACF commands to fix the configuration error and then execute the RACF IRRVERLD utility to retry the software integrity test.

The integrity of the module is verified by checking an RSA/SHA-256-based digital signature of the module's binary prior to being utilized in FIPS 140-2 compliant mode. Initialization will only succeed if the module's signature is verified successfully. The module signature is generated during the final phase of the build process. The integrity verification involves loading the IRRPVERS module twice into different storage locations. The first copy verifies the integrity of the second copy. Verification involves verifying the digital signature (RSA 2048 bits with SHA256) inside the module with the to-be-verified data of the loaded module. Since the two module copies are identical, verifying the integrity of the second copy implies that the integrity of the first copy is also verified. Once verified, the second copy is removed from memory. Any failures during the integrity check result in transition back to the IRRPVERS uninitialized state thus preventing any cryptographic function from being performed..

Per section 9.3 of FIPS 140-2 (KAT for Algorithms used in Integrity Test Technique) it is not necessary for IRRPVERS to perform a known answer test because its cryptographic functionality is tested by the module integrity test.

The module tests the following cryptographic algorithms:

CPACF – SHA-256

Software – RSA Signature Verify

Invoking FIPS 140-2 self-tests on demand

If the RACF IRRPVERS integrity test has previously completed without error, a system reboot is required for the RACF IRRPVERS module to repeat the module integrity test on demand. If the RACF IRRPVERS integrity test has not previously completed successfully, the test can be executed on demand by executing the IRRVERLD utility.

Application Programming Interfaces (APIs)

The following Services (APIs) in Table 8: RACF Signature Verification Module Services (API) can be executed by the user. The approved/allowed services used by the APIs are:

- RSA (1024 and 2048 bits) signature verification (SHA-256)

Verb	***Service Name***	***Description***
R_PgmSignVer (IRRSPS00)	Program Sign and Verify	R_PgmSignVer service provides the function required to verify a z/OS program object signature.

Table 8: RACF Signature Verification Module Services (API)

Glossary

API	Application Programming Interface
CPACF	CP Assist for Cryptographic Function DES/TDES Enablement Feature 3863 , clear key on-chip accelerator integrated into mainframe processors. CPACF functionality is restricted to symmetric and hashing operations
CP	Central Processor
COP	Coprocessor unit
KAT	Known Answer Test
OS	Operating System
ServerPac	Prepackaged version of the z/OS Operating System

References

[1] National Institute of Standards and Technology, Security Requirements for Cryptographic Modules (FIPS 140-2), 2002

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

ㅎ IBM

ㅎ RACF

ㅎ z13

ㅎ z/OS