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)*

Questa pagina è lasciata intenzionalmente vuota

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

Rapporto di Certificazione

IBM RACF for z/OS Version 2 Release 3

OCSI/CERT/ATS/09/2018/RC

Versione 1.0

16 settembre 2019

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	16/09/2019

2 Indice

3 Elenco degli acronimi

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
ODV	Oggetto Della Valutazione
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

SVC Supervisor Call

SVT System Verification Tests

TCP/IP Transmission Control Protocol/Internet Protocol

TDS Traguardo di Sicurezza

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 Riferimenti

4.1 Criteri e normative

[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 Documenti tecnici

[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

[TDS] 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 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La versione corrente dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL 2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su http://www.commoncriteriaportal.org.

Il logo CCRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito CCRA fino a EAL2.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "IBM RACF for z/OS Version 2 Release 3", sviluppato dalla società International Business Machines Corp. (IBM).

RACF for z/OS Version 2 Release 3 (di seguito indicato anche come RACF V2R3 o RACF) è il componente del sistema operativo z/OS che viene richiamato all'interno di z/OS da qualsiasi componente che necessiti di autenticare un utente, controllare l'accesso alle risorse protette e gestire gli attributi di sicurezza e i diritti di accesso degli utenti.

La valutazione è stata condotta in accordo ai requisiti stabiliti dallo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo di Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per il livello di garanzia EAL5, con aggiunta di ALC_FLR.3, in conformità a quanto indicato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B – Configurazione valutata di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri di valutazione Common Criteria – ISO/IEC 15408 ([CC1], [CC2], [CC3]) e dalle procedure indicate dal Common Criteria Recognition Arrangement [CCRA] e che nessuna vulnerabilità sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione riassume l'esito della valutazione di sicurezza del prodotto "IBM RACF for z/OS Version 2 Release 3" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

I potenziali acquirenti sono quindi tenuti a consultare il presente Rapporto di Certificazione congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	IBM RACF for z/OS Version 2 Release 3
Traguardo di Sicurezza	Security Target for IBM RACF for z/OS V2R3, Version 5.5 [TDS]
Livello di garanzia	EAL5 con aggiunta di ALC_FLR.3
Fornitore	IBM Corporation
Committente	IBM Corporation
LVS	atsec information security GmbH
Versione dei CC	3.1 Rev. 5
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	27 novembre 2018
Data di fine della valutazione	28 giugno 2019

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel presente Rapporto di Certificazione e a condizione che siano rispettate le ipotesi sull'ambiente descritte nel Traguardo di Sicurezza [TDS].

7.3 Prodotto valutato

In questo capitolo vengono sintetizzate le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'ODV è il prodotto IBM RACF for z/OS Version 2 Release 3 caratterizzato dai seguenti elementi:

- RACF for z/OS V2R3 come parte integrante di z/OS Version 2 Release 3 (z/OS V2.3, program number 5650-ZOS) Common Criteria Evaluated Base Package

RACF è il componente che viene richiamato all'interno di z/OS da qualsiasi componente che necessiti di autenticare un utente, controllare l'accesso alle risorse protette e gestire gli attributi di sicurezza e i diritti di accesso degli utenti (RACF sta per Resource Access Control Facility).

L'ODV fornisce funzionalità di identificazione e autenticazione degli utenti mediante diversi meccanismi di autenticazione, controllo di accesso sia discrezionale (DAC), sia vincolato (MAC) con supporto per la sicurezza basata su etichette, funzionalità di audit, funzioni di gestione della sicurezza, firma e verifica dei programmi e protezione del TSF.

Una descrizione più dettagliata delle funzioni di sicurezza dell'ODV è riportata nel cap. 7.3.2.3.

7.3.1 Architettura dell'ODV

7.3.1.1 Panoramica generale dell'ODV

L'ODV è il componente RACF del sistema operativo z/OS progettato per fornire funzionalità di autenticazione e di gestione degli accessi. RACF gestisce sia gli attributi di sicurezza dell'utente, sia gli attributi di gestione dell'accesso nel proprio database. Gli utenti sono rappresentati in RACF dai profili d'utente, mentre le risorse protette sono rappresentate dai profili delle risorse. Gli utenti possono essere membri di gruppi, ognuno rappresentato da un profilo di gruppo.

I profili delle risorse sono strutturati in classi che rappresentano i diversi tipi di risorse. All'interno di una classe un singolo profilo è rappresentato dal nome della risorsa, che è univoco all'interno della sua classe. Il gestore delle risorse interroga RACF ogni volta che deve verificare i diritti di accesso di un utente ad una risorsa. In questa *query* vengono specificate la classe della risorsa, il nome della risorsa all'interno della classe, il tipo di accesso richiesto e la rappresentazione interna dell'utente che richiede l'accesso. RACF viene richiamato anche nel caso in cui un componente interno di z/OS ha la necessità di autenticare un utente. In questo caso il componente di z/OS fornisce a RACF svariati parametri, tra i quali l'identità dell'utente, le credenziali di autenticazione presentate, il nome del componente che richiede l'autenticazione dell'utente. RACF provvede ad autenticare l'utente sulla base di queste informazioni e, in caso di verifica positiva, crea un blocco di controllo che rappresenta l'utente con gli attributi di sicurezza assegnati. Questo blocco di controllo viene successivamente utilizzato quando un componente di z/OS richiama RACF per verificare i diritti di accesso.

RACF fornisce interfacce che consentono la gestione di profili d'utente, certificati digitali assegnati agli utenti, profili di gruppo, profili di risorse, diritti di accesso, etichette di sicurezza e attributi generici di RACF. RACF fornisce altresì un'interfaccia che può essere richiamata dai componenti di z/OS per generare un record di audit di sicurezza.

Nota: la funzionalità RACF Remote Sharing Facility (RRSF) non è considerata parte di questa valutazione e pertanto non deve essere utilizzata nel sistema in configurazione certificata.

7.3.1.2 Metodi d'uso dell'ODV

RACF è progettato per essere utilizzato dai componenti di z/OS per eseguire l'autenticazione degli utenti, convalidare l'accesso di un utente a una risorsa, effettuare l'audit di eventi critici per la sicurezza e gestire i profili di RACF, i diritti di accesso alle risorse e i parametri di sicurezza di RACF. RACF fornisce inoltre un'interfaccia per estrarre informazioni sul proprio stato. Quest'interfaccia di programmazione è implementata dalla macro RACROUTE. RACF verifica se l'applicazione chiamante ha il diritto di utilizzare la funzione chiamata. Inoltre, RACF fornisce un'interfaccia a riga di comando che può essere utilizzata direttamente dagli utenti specificamente autorizzati per eseguire operazioni di gestione.

Il Traguardo di Sicurezza [TDS] specifica due modalità operative: una modalità "normale", in cui le funzionalità di sicurezza con etichette (*labeled security*) non sono configurate e una modalità chiamata Labeled Security Mode, in cui la sicurezza con etichette è configurata come descritto. Nella modalità Labeled Security Mode sono attive funzionalità di sicurezza aggiuntive, contrassegnate in questo documento con la dicitura Labeled Security Mode. Si noti che quando le funzioni di sicurezza con etichette sono configurate in modo diverso da quanto specificato nel Traguardo di Sicurezza, la funzionalità di sicurezza definita per la modalità "normale" continua a funzionare, ma possono essere imposte ulteriori restrizioni a causa del modo in cui sono configurate le funzioni per la sicurezza con etichette.

7.3.2 Caratteristiche di sicurezza dell'ODV

7.3.2.1 Politica di sicurezza

La politica di sicurezza dell'ODV è espressa dall'insieme dei Requisiti Funzionali di Sicurezza (SFR) implementati dallo stesso. Essa copre i seguenti aspetti:

- Identificazione e Autenticazione degli utenti.
- Controllo di Accesso Discrezionale (DAC).
- Controllo di Accesso Vincolato (MAC) e supporto per la sicurezza basata su etichette (Labeled Security Mode).
- Funzionalità di Audit.
- Gestione della sicurezza.
- Firma e verifica dei programmi.
- Protezione del TSF.

Queste funzioni di sicurezza primarie sono supportate dalle proprietà di separazione dei domini e di accesso con mediazione dei riferimenti delle altre porzioni del sistema operativo z/OS, che assicurano che le funzioni di RACF siano invocate quando richiesto e

non possano essere aggirate. RACF stesso è protetto dall'architettura del sistema operativo z/OS da manomissioni non autorizzate alle sue funzioni e al suo database.

7.3.2.2 Obiettivi di sicurezza dell'ambiente operativo

Le ipotesi definite nel Traguardo di Sicurezza [TDS] ed alcuni aspetti delle minacce e delle politiche di sicurezza organizzative non sono coperte dall'ODV stesso. Tali aspetti implicano che specifici obiettivi di sicurezza debbano essere soddisfatti dall'ambiente operativo dell'ODV. In particolare, in tale ambito i seguenti aspetti sono da considerare di rilievo:

- I responsabili dell'ODV sono competenti e fidati, in grado di gestire l'ODV e la sicurezza delle informazioni in esso contenute.
- I responsabili dell'ODV devono stabilire e attuare procedure per garantire che le informazioni siano protette in modo adeguato.
- I responsabili dell'ODV devono stabilire e attuare procedure per garantire che i componenti dell'ODV siano distribuiti, installati e configurati in modo sicuro a supporto dei meccanismi di sicurezza forniti dall'ODV.
- Gli utenti autorizzati dell'ODV devono garantire che le funzionalità di diagnostica completa fornite dal prodotto vengano invocate ad ogni intervallo di manutenzione programmato.
- I responsabili dell'ODV devono garantire che le parti dell'ODV fondamentali per l'applicazione della politica di sicurezza siano protette da attacchi fisici che possono compromettere gli obiettivi di sicurezza IT.
- I responsabili dell'ODV devono garantire che siano fornite procedure e/o meccanismi per assicurare il ripristino dell'operatività a seguito di errori di sistema o altre interruzioni senza che la sicurezza venga compromessa.
- Il sistema operativo z/OS fornisce i meccanismi per mantenere la separazione degli spazi di indirizzamento di RACF da qualsiasi altro spazio di indirizzamento non attendibile e per proteggere i programmi e i dati di RACF da qualsiasi accesso non controllato da parte di entità non attendibili.
- I responsabili del sistema operativo in cui è integrato l'ODV devono garantire che siano installati solo programmi che siano completamente affidabili.

Per una descrizione completa degli obiettivi di sicurezza per l'ambiente dell'ODV, si faccia riferimento al capitolo 4.2 del Traguardo di Sicurezza [TDS].

7.3.2.3 Funzioni di sicurezza

Le funzionalità di sicurezza dell'ODV sono descritte in dettaglio nel capitolo 1.4.2 del Traguardo di Sicurezza [TDS]. Di seguito sono riassunte le principali caratteristiche di sicurezza del prodotto che sono state oggetto di valutazione:

- **Identificazione e Autenticazione**: RACF fornisce supporto per l'identificazione e l'autenticazione degli utenti mediante i seguenti meccanismi:

- Un ID utente alfanumerico di RACF e una password o *passphrase* cifrata dal sistema.

- Un ID utente alfanumerico di RACF e un PassTicket, che è un sostituto della password generato crittograficamente che comprende l'ID utente, il nome dell'applicazione richiesta e la data e l'ora correnti.

- Un certificato digitale x.509v3 presentato ad un'applicazione server nell'ambiente dell'ODV che utilizza System SSL o TCP/IP Application Transparent TLS (AT-TLS) per fornire l'autenticazione client basata su TLS o SSLv3, che viene quindi "mappato" (usando le funzioni dell'ODV) dall'applicazione server o da AT-TLS su di un ID utente di RACF.

- Un ticket Kerberos™ v5 presentato ad un *application server* nell'ambiente dell'ODV che supporta il meccanismo Kerberos, che viene mappato da tale applicazione tramite i servizi di programmazione GSS-API. L'ODV fornisce anche funzioni che consentono all'*application server* di convalidare il ticket Kerberos e quindi l'autenticazione dell'entità. L'*application server* quindi traduce (o mappa) l'entità Kerberos in un ID utente di RACF.

Le funzioni di sicurezza dell'ODV autenticano l'identità fornita dall'utente verificando la password/*passphrase* (o altro meccanismo tra quelli sopra elencati) e restituendo il risultato al programma attendibile che ha richiamato le funzioni di RACF per l'identificazione e l'autenticazione dell'utente. In caso di fallimento del processo di identificazione e autenticazione dell'utente, spetta al programma chiamante decidere cosa fare. Quando un utente viene identificato e autenticato correttamente, RACF crea blocchi di controllo contenenti gli attributi di sicurezza dell'utente gestiti da RACF. Tali blocchi di controllo vengono utilizzati in seguito quando un gestore delle risorse richiama RACF per determinare il diritti di accesso dell'utente alle risorse o quando l'utente richiama funzioni di RACF che richiedono all'utente di disporre di privilegi specifici gestiti da RACF.

- **Controllo di Accesso Discrezionale (DAC)**: RACF implementa le funzioni che consentono ai gestori delle risorse all'interno di z/OS di controllare l'accesso alle risorse che devono proteggere. Le risorse protette da RACF rientrano in due categorie, sulla base dei meccanismi utilizzati all'interno di RACF per descriverle: Standard (ad es., set di dati MVS o risorse generali in classi definite da RACF o dall'amministratore di sistema) e UNIX (ad es., file e directory UNIX e oggetti IPC istanziati da un *file system* UNIX). Le regole DAC consentono ai gestori delle risorse di differenziare l'accesso degli utenti alle risorse in base a diversi tipi di accesso.

- **Controllo di Accesso Vincolato (MAC) e supporto per la sicurezza basata su etichette**: oltre al DAC, RACF fornisce le funzioni MAC necessarie per la modalità di sicurezza Labeled Security Mode, che impone ulteriori restrizioni di accesso al flusso di informazioni basate sulla classificazione di sicurezza. Gli utenti e le risorse possono avere un'etichetta di sicurezza specificata nel loro profilo. Le etichette di sicurezza contengono una classificazione gerarchica (livello di sicurezza) che specifica la sensibilità (ad es.: pubblico, uso interno o segreto) e zero o più categorie di sicurezza non gerarchiche (ad es.: PROJECTA o PROJECTB). Il controllo di accesso applicato dall'ODV garantisce che gli utenti possano

accedere in lettura alle informazioni etichettate solo se le loro etichette di sicurezza dominano l'etichetta delle informazioni e che possano accedere in scrittura ai contenitori di informazioni etichettate solo se l'etichetta del contenitore domina l'etichetta del soggetto, implementando così il modello di Bell-LaPadula per il controllo del flusso di informazioni. Il sistema può anche essere configurato per consentire il *write-down* per determinati utenti autorizzati.

- **Funzionalità di Audit**: l'ODV fornisce una funzionalità di audit che consente di generare record di audit per eventi critici di sicurezza. RACF offre una serie di funzioni di log e reportistica che consentono agli utenti proprietari delle risorse e agli utenti con ruolo auditor di identificare gli utenti che tentano di accedere alle risorse. I record di audit vengono generati da RACF e inviati a un altro componente di z/OS (SMF - System Management Facilities), che li raccoglie in un'*audit trail*.
  RACF genera sempre record di controllo per eventi quali tentativi non autorizzati di accesso al sistema o modifiche allo stato del database di RACF. L'amministratore della sicurezza, gli auditor e altri utenti con opportuna autorizzazione possono configurare quali eventi di sicurezza opzionali aggiuntivi devono essere registrati. Oltre a scrivere i record nell'*audit trail*, è possibile inviare messaggi alla console di sicurezza per avvisare immediatamente gli operatori delle violazioni delle policy rilevate. RACF fornisce record SMF per tutte le risorse protette da RACF ("tradizionali" o basate su UNIX z/OS).
  Per la reportistica, gli auditor possono scaricare i dati SMF completi, o solo porzioni selezionate di essi, per ulteriori analisi in formati leggibili dall'uomo e possono, se necessario, caricare i dati in una *query* o in uno strumento di reportistica come DFSORT™.

- **Gestione della sicurezza**: RACF fornisce una serie di comandi e opzioni per gestire in modo adeguato le funzioni di sicurezza dell'ODV. Inoltre, RACF offre la possibilità di gestire utenti, gruppi di utenti, profili di risorse generali e opzioni SETROPTS di RACF.
  RACF riconosce diversi ruoli autoritativi che possono eseguire le diverse attività di gestione relative alla sicurezza dell'ODV:

  - Le opzioni di sicurezza generali sono gestite dagli amministratori della sicurezza.

  - La gestione degli attributi MAC viene eseguita dagli amministratori della sicurezza in modalità Labeled Security Mode.

  - La gestione degli utenti e dei relativi attributi di sicurezza viene eseguita dagli amministratori della sicurezza. La gestione dei gruppi e, fino a un certo limite, degli utenti può essere delegata ad amministratori della sicurezza dei gruppi.

  - Gli utenti possono modificare la propria password o *passphrase*, il loro gruppo predefinito e il loro nome utente (ma non il loro ID utente).

  - Gli utenti possono scegliere le proprie etichette di sicurezza al login, per alcuni metodi di login, in modalità Labeled Security Mode (Nota: questo si applica anche alla modalità normale nel caso un cui gli amministratori hanno attivato l'elaborazione delle etichette di sicurezza).

- Gli auditor gestiscono i parametri del sistema di audit (ad es., l'elenco degli eventi controllati) e possono analizzare l'*audit trail*.

- Gli amministratori della sicurezza possono definire quali record di audit vengono acquisiti dal sistema.

- I diritti di accesso discrezionale alle risorse protette sono gestiti dai proprietari dei profili applicabili (o oggetti UNIX) o dagli amministratori della sicurezza.

- **Firma e verifica dei programmi**: RACF fornisce i servizi di supporto alla firma e alla verifica della firma degli oggetti programma di z/OS. La funzione può essere utilizzata sia per firmare un programma sia per verificare la firma di un programma. La funzione è pensata per essere utilizzata dal Program Binder di z/OS (per la firma di oggetti programma) e dal Loader di z/OS (per la verifica della firma di un oggetto programma). La firma viene generata utilizzando SHA-256 come funzione *hash* e RSA come algoritmo di crittografia a chiave pubblica. La dimensione massima della chiave RSA è di 4096 bit.

- **Protezione del TSF (fornita dall'ambiente di RACF)**: La protezione del TSF si basa su diversi meccanismi di protezione forniti dalla macchina astratta sottostante e dal sistema operativo z/OS:

  - Le istruzioni privilegiate del processore sono disponibili solo per i programmi in esecuzione nella modalità supervisore del processore.

  - Le istruzioni semi-privilegiate sono disponibili solo per i programmi in esecuzione in un ambiente di esecuzione stabilito e autorizzato dal TSF.

  - Durante l'operatività, tutti gli spazi di indirizzamento, nonché i dati e i *task* in essi contenuti, sono protetti dai meccanismi di protezione della memoria della macchina astratta sottostante.

  - z/OS protegge lo spazio di indirizzamento di RACF e le funzioni di RACF da accessi non autorizzati e z/OS o RACF stesso assicurano che un'entità che richiama i servizi di RACF disponga dei privilegi hardware o di z/OS (ad es., modalità supervisore, chiave PSW, autorizzazione APF) necessari per invocare il servizio.

  La gestione dello spazio di indirizzamento di z/OS garantisce che i programmi in esecuzione nella modalità utente del processore (*problem state*) non possano accedere alla memoria protetta o alle risorse che appartengono ad altri spazi di indirizzamento.
  L'accesso ai servizi di sistema, ad esempio tramite le istruzioni di tipo Supervisor Call (SVC) o Program Call (PC), è controllato da z/OS, che richiede che i soggetti che desiderano svolgere attività rilevanti per la sicurezza siano autorizzati in modo appropriato.
  I componenti hardware e firmware che forniscono la macchina astratta per l'ODV devono essere protetti fisicamente da accessi non autorizzati.
  L'ambiente operativo dell'ODV fornisce agli amministratori autorizzati gli strumenti per verificare il corretto funzionamento della macchina astratta sottostante.
  Oltre al meccanismo di protezione della macchina astratta sottostante, per

proteggere il TSF z/OS utilizza anche meccanismi software come la Authorized Program Facility (APF) o privilegi specifici per i programmi nell'ambiente UNIX System Services.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto viene fornita al cliente finale insieme al prodotto. Questa documentazione contiene le informazioni richieste per l'installazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguiti gli ulteriori obblighi o note per l'utilizzo sicuro dell'ODV contenuti nel capitolo 8.2 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] non dichiara conformità ad alcun Profilo di Protezione.

7.6 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati dai CC Parte 3 [CC3] ed includono tutti i requisiti del pacchetto EAL5 con l'aggiunta di ALC_FLR.3.

Tutti i Requisiti Funzionali (SFR) sono stati derivati direttamente o per estensione dai CC Parte 2 [CC2]. In particolare, il Traguardo di Sicurezza [TDS] include i seguenti componenti estesi:

- **FIA_USB.2 Enhanced user-subject binding**: FIA_USB.2 è analogo a FIA_USB.1, tranne per il fatto che aggiunge la possibilità di specificare regole in base alle quali gli attributi di sicurezza del soggetto sono derivati anche da dati del TSF diversi dagli attributi di sicurezza dell'utente. FIA_USB.2 è stato tratto dal PP "Operating System Protection Profile" (OSPP).

- **FAU_GEN_SUB.1 Subset audit data generation**: questo componente esteso definisce un sottoinsieme del componente FAU_GEN.1 come definito nella parte 2 dei CC. L'uso di questo componente esteso si è reso necessario in quanto RACF utilizza le interfacce fornite dal componente SMF di z/OS per i componenti attendibili che richiedono di archiviare i loro record di audit nell'*audit trail* comune fornita da z/OS.

Per una descrizione dettagliata delle proprietà dei componenti estesi, consultare il cap. 5 del Traguardo di Sicurezza [TDS].

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione e le note applicative, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, i Requisiti Funzionali di Sicurezza (SFR) e le funzioni di sicurezza che realizzano gli obiettivi stessi.

7.7 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement [CCRA].

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS atsec information security GmbH.

L'attività di valutazione è terminata in data 28 giugno 2019 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [ETR] che è stato approvato dall'Organismo di Certificazione il 30 luglio 2019. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in Appendice B – Configurazione valutata. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

8 Esito della valutazione

8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [ETR] prodotto dall'LVS atsec information security GmbH e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "IBM RACF for z/OS Version 2 Release 3" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL5, con l'aggiunta di ALC_FLR.3, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B – Configurazione valutata.

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia EAL5, con l'aggiunta di ALC_FLR.3.

Classi e componenti di garanzia		**Verdetto**
Security Target evaluation	**Classe ASE**	Positivo
Conformance claims	ASE_CCL.1	Positivo
Extended components definition	ASE_ECD.1	Positivo
ST introduction	ASE_INT.1	Positivo
Security objectives	ASE_OBJ.2	Positivo
Derived security requirements	ASE_REQ.2	Positivo
Security problem definition	ASE_SPD.1	Positivo
TOE summary specification	ASE_TSS.1	Positivo
Development	**Classe ADV**	Positivo
Security architecture description	ADV_ARC.1	Positivo
Complete semi-formal functional specification with additional error information	ADV_FSP.5	Positivo
Implementation representation of the TSF	ADV_IMP.1	Positivo
Well-structured internals	ADV_INT.2	Positivo
Semiformal modular design	ADV_TDS.4	Positivo
Guidance documents	**Classe AGD**	Positivo
Operational user guidance	AGD_OPE.1	Positivo
Preparative procedures	AGD_PRE.1	Positivo
Life cycle support	**Classe ALC**	Positivo
Production support, acceptance procedures and automation	ALC_CMC.4	Positivo
Development tools CM coverage	ALC_CMS.5	Positivo
Delivery procedures	ALC_DEL.1	Positivo

Classi e componenti di garanzia		Verdetto
Identification of security measures	ALC_DVS.1	Positivo
Developer defined life-cycle model	ALC_LCD.1	Positivo
Compliance with implementation standards	ALC_TAT.2	Positivo
Systematic flaw remediation	*ALC_FLR.3*	Positivo
Tests	**Classe ATE**	Positivo
Analysis of coverage	ATE_COV.2	Positivo
Testing: modular design	ATE_DPT.3	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Methodical vulnerability analysis	AVA_VAN.4	Positivo

Tabella 1- Verdetti finali per i requisiti di garanzia

8.2 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 6 (Dichiarazione di certificazione)

Si raccomanda ai potenziali acquirenti del prodotto "IBM RACF for z/OS Version 2 Release 3" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo all'ambiente di sicurezza specificato nel capitolo 4.2 del Traguardo di Sicurezza [TDS]. Si consiglia ai potenziali acquirenti di verificare la rispondenza ai requisiti identificati e di prestare attenzione alle raccomandazioni contenute in questo Rapporto.

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella sua configurazione valutata. In particolare, l'Appendice A – Indicazioni per l'uso sicuro del prodotto del presente Rapporto include una serie di raccomandazioni relative alla consegna, all'inizializzazione, all'installazione e all'utilizzo sicuro del prodotto, in accordo con la documentazione di guida fornita con l'ODV ([MLSGUIDE], [RACF.SAG], [RACF.UG]).

Si assume che l'ODV funzioni in modo sicuro qualora vengano rispettate le ipotesi sull'ambiente operativo descritte nel cap. 3.3 del Traguardo di Sicurezza [TDS]. In particolare, si assume che gli amministratori dell'ODV siano adeguatamente addestrati al corretto utilizzo dell'ODV e scelti tra il personale fidato dell'organizzazione. L'ODV non è realizzato per contrastare minacce provenienti da amministratori inesperti, malfidati o negligenti.

Occorre inoltre notare che la sicurezza dell'operatività dell'ODV è condizionata al corretto funzionamento delle piattaforme software e hardware su cui è installato l'ODV e di tutti i sistemi IT esterni attendibili sui quali l'ODV si basa per supportare la realizzazione della

sua politica di sicurezza. Le specifiche dell'ambiente operativo sono descritte nel Traguardo di Sicurezza [TDS].

9 Appendice A – Indicazioni per l'uso sicuro del prodotto

La presente appendice riporta considerazioni particolarmente rilevanti per il potenziale acquirente del prodotto.

9.1 Consegna dell'ODV

L'ODV è composto unicamente da software ed è accompagnato dalla documentazione di guida. L'ODV è parte integrante del sistema operativo z/OS e può essere ottenuto solo come parte del pacchetto "z/OS Version 2 Release 3 Common Criteria Evaluated Base".

In Tabella 2 sono elencati gli elementi che comprendono i diversi componenti di z/OS, inclusi il software e le guide. Alcuni elementi non di rilievo per RACF sono stati omessi.

N.	Tipo	Identificativo	Release	Metodo di consegna
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). Questo pacchetto contiene l'ODV.	V2R3	Nastro
2	DOC	z/OS V2.3 Program Directory	GI11-9848-02	Copia cartacea
3	DOC	z/OS V2.3 Documentation Collection Codici *hash* per il 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	Copia cartacea
5	DOC	Memo to Customers of z/OS V2.3 Common Criteria Evaluated Base	n/a	Copia cartacea
6	DOC	z/OS V2.3 Planning for Multilevel Security and the Common Criteria; Document No. GA32-0891-30 Codice *hash* del documento: **SHA256**: 48cee926a44883fd7cb93b49e995b7f19f5da309b48a24aaef917a9738001b8f		
Supporti aggiuntivi				
14	SW	PTF per i seguenti APAR (richiesti). Si noti che l'elenco include APAR non direttamente applicabili all'ODV ma al sistema operativo z/OS di base. Gli APAR e i rispettivi PTF di rilievo per l'ODV sono indicati in **grassetto**: • **OA52110 (PTF UA93049)** • OA52192 (PTF UA93490) • OA52722 (PTF UA93924)	n/a	Formato elettronico

[1] Il "program number" (o "product number") è un'identificazione tecnica del prodotto "z/OS" da parte di IBM. È utilizzato per effettuare gli ordini e per la gestione delle licenze e non identifica in modo univoco l'ODV. La stringa z/OS Version 2 Release 3 identifica in modo univoco l'ODV z/OS.

N.	Tipo	Identificativo	Release	Metodo di consegna
		• OA52830 (PTF UA92871) • **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) Inoltre, è necessario ottenere i seguenti APAR/PTF: **OA57638 (PTF UA99514, UA99513)**. Questi PTF devono essere scaricati in formato elettronico da ShopzSeries (https://www.ibm.com/software/shopzseries)		

Tabella 2- Materiali consegnabili dell'ODV

La versione certificata di z/OS contenente l'ODV può essere ordinata contattando un rappresentante di vendita di IBM o tramite l'applicazione Web ShopzSeries (http://www.ibm.com/software/shopzseries). Per effettuare un ordine tramite i servizi Internet sicuri di IBM, i clienti debbono avere un *account* con nome utente e password. La registrazione di un account a sua volta richiede di essere in possesso di un ID cliente di IBM valido.

La consegna dei nastri e della documentazione avviene in un unico pacchetto, prodotto appositamente per il singolo cliente e spedito tramite corriere. Il software aggiuntivo di mantenimento deve essere scaricato successivamente dal cliente dal sito Web ShopzSeries, seguendo le istruzioni fornite col pacchetto.

La procedura di download delle guide dell'ODV (voce num. 3 in Tabella 2) è descritta in [MLSGUIDE]. Il cliente scarica il pacchetto contenente le guide da un server FTP di IBM e ne verifica l'autenticità utilizzando i codici *hash* forniti in [MLSGUIDE] o in questo rapporto.

9.2 Identificazione dell'ODV

I supporti e i documenti consegnati al cliente sono etichettati con i rispettivi numeri di prodotto, documento e versione indicati in Tabella 2 e possono essere controllati dagli utenti che installano il sistema.

Il riferimento dell'ODV può essere verificato dall'amministratore durante la fase di Initial Program Load (IPL) di z/OS (che contiene l'ODV) nel momento in cui l'identificativo del sistema viene visualizzato sulla console. L'operatore può anche utilizzare il comando D IPLINFO per visualizzare la versione z/OS. Va verificato che la stringa "z/OS 02.03.00" compaia tra le altre informazioni.

9.3 Installazione, inizializzazione ed utilizzo sicuro dell'ODV

L'ODV è parte integrante del sistema operativo z/OS e può essere installato solo come parte della configurazione certificata di z/OS.

L'installazione e la configurazione dell'ODV debbono essere effettuate seguendo le istruzioni contenute nelle apposite sezioni della documentazione di guida fornita al cliente con il prodotto.

In particolare, i seguenti documenti contengono informazioni per l'inizializzazione sicura dell'ODV e la preparazione del suo ambiente operativo in conformità con gli obiettivi di sicurezza specificati nel Traguardo di Sicurezza [TDS]:

- 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 Appendice B – Configurazione valutata

La presente certificazione copre la seguente configurazione dell'ODV.

Il pacchetto "z/OS Version 2 Release 3 Common Criteria Evaluated Base" deve essere installato secondo le indicazioni incluse con il supporto e configurato seguendo le istruzioni fornite nel cap. 7 ("The evaluated configuration for the Common Criteria") del documento z/OS Planning for Multilevel Security and the Common Criteria [MLSGUIDE]. Inoltre, devono essere installati tutti i PTF necessari, elencati alla voce num. 14 in Tabella 2.

Nell'installazione si può scegliere di non utilizzare uno qualsiasi degli elementi forniti all'interno del ServerPac, ma è necessario installare, configurare e utilizzare l'ODV, ossia l'elemento z/OS Security Server (RACF).

Inoltre, possono essere aggiunti software esterni all'ODV senza influire sulle caratteristiche di sicurezza del sistema, a patto che non possano essere eseguiti:

- in modalità supervisore;
- come APF-authorized;
- in chiave da 0 a 7;
- con UID(0);
- con autorità per le risorse BPX.DAEMON, BPX.SERVER o BPX.SUPERUSER della classe FACILITY;
- con autorità per le risorse UNIXPRIV.

Questo esclude in maniera esplicita:

- la sostituzione di qualsiasi elemento nel ServerPac che fornisce funzioni di sicurezza rilevanti per questa valutazione con altri prodotti di terze parti;
- l'installazione di punti di uscita dal sistema (*system exit*) che girano autorizzati (in modalità supervisore, in chiave di sistema o APF-authorized), ad eccezione dell'uscita predefinita ICHPWX11 e della relativa routine IRRPHREX;
- l'installazione di *plugin* di IBM Tivoli Directory Server che non sono stati valutati;
- l'utilizzo della Authorized Caller Table (ICHAUTAB) in RACF per consentire a programmi non autorizzati di invocare RACROUTE REQUEST=VERIFY (RACINIT) o RACROUTE REQUEST=LIST (RACLIST).

Nota: *La configurazione valutata del software non viene invalidata installando ed eseguendo altri componenti adeguatamente certificati che potrebbero girare autorizzati. Tuttavia, la valutazione di tali componenti deve dimostrare che il componente e le politiche*

di sicurezza implementate dal componente non indeboliscono le politiche di sicurezza descritte in questo documento.

RACF:

- Non utilizzare la funzione di condivisione remota di RACF (RRSF) in modalità remota. Se si utilizza RRSF in modalità locale, assicurarsi che non possa essere utilizzata la funzione di *command direction* agendo in uno dei modi seguenti:
    - assicurarsi che la classe RRFSFDATA non sia attiva;
    - definire il profilo DIRECT.* nella classe RRSFDATA con UACC(NONE) e nessun utente nella lista di accesso.
- Non utilizzare l'autenticazione a più fattori. È possibile disabilitare l'uso dell'autenticazione a più fattori rendendo inattiva la classe MFADEF.

Qualsiasi client consegnato con il prodotto che viene eseguito con i privilegi dell'utente deve essere utilizzato con attenzione, in quanto il TSF non può proteggere quei client da programmi potenzialmente ostili. Le password/*passphrase* inserite dall'utente in uno di questi programmi client, che vengono quindi inviate al server di destinazione per autenticare l'utente, potrebbero essere potenzialmente intercettate o falsificate da programmi ostili in esecuzione nello spazio di indirizzamento dell'utente. Questi programmi client includono telnet, TN3270, ftp, r-command, ssh, tutte le utility LDAP e le utility di amministrazione Kerberos che richiedono all'utente di inserire la propria password/*passphrase*. Quando si utilizzano tali programmi client, l'utente deve assicurarsi che durante la sua sessione non sia in esecuzione alcun programma non attendibile potenzialmente ostile.

I seguenti elementi e componenti non possono essere utilizzati in un sistema certificato, in quanto violano le politiche di sicurezza indicate nel Traguardo di Sicurezza [TDS] o perché non sono stati inclusi nella configurazione valutata a causa di vincoli di tempo e risorse della valutazione. Poiché fanno parte del sistema di base, non devono essere configurati per l'uso o devono essere disattivati, come descritto nel capitolo 7 di [MLSGUIDE]:

- Tutti gli elementi Bulk Data Transfer (BDT): BDT, BDT File-to-File e BDT Systems Network Architecture (SNA) NJE.
- I componenti DFS™ Server Message Block (SMB) dell'elemento Distributed File Service.
- Infoprint® Server.
- JES3.
- IBM Ported Tools for z/OS HTTP Server V7.0.

Inoltre, le seguenti funzionalità non possono essere utilizzate nella configurazione certificata:

- Il componente Advanced Program-to-Program Communication/Multiple Virtual Storage (APPC/MVS) del BCP.
- Il DFSMS Object Access Method per applicazioni di tipo *content management*.
- la funzione di condivisione remota di RACF in modalità remota.
- JES2 NJE con comunicazione via TCP/IP. Nella configurazione certificata JES2 NJE deve utilizzare SNA o BSC.
- La funzionalità JES2 Execution Batch Monitor (XBM).
- La maggior parte delle funzioni di Enterprise Identity Mapping (EIM). Per i dettagli, si faccia riferimento al manuale z/OS Planning for Multilevel Security and the Common Criteria [MLSGUIDE].

11 Appendice C –Attività di Test

Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL5, con l'aggiunta di ALC_FLR.3, tali attività prevedono tre passi successivi:

- valutazione in termini di copertura e livello di approfondimento dei test eseguiti dal Fornitore;
- esecuzione di test funzionali indipendenti da parte dei Valutatori;
- esecuzione di test di intrusione da parte dei Valutatori.

11.1 Configurazione per i Test

Il Traguardo di Sicurezza [TDS] richiede che i pacchetti software che compongono l'ODV siano eseguiti su una macchina astratta che implementa l'interfaccia della macchina z/Architecture come definita in "z/Architecture Principles of Operation" [ZARCH]. Le piattaforme hardware che implementano questa macchina astratta sono:

- IBM zEnterprise zEC12/BC12 con attiva la CPACF DES/TDES Enablement Feature 3863 attiva, con scheda Crypto Express3 o Crypto Express4S e con o senza la zEnterprise BladeCenter Extension (zBX).
- IBM z13/z13s con attiva la CPACF DES/TDES Enablement Feature 3863, con scheda Crypto Express4, Crypto Express4S o Crypto Express5S, con o senza la zEnterpriss BladeCenter Extension (zBX).
- IBM z14 con attiva la CPACF DES/TDES Enablement Feature 3863, con scheda Crypto Express5S o Crypto Express6S.

Si noti che le schede Crypto Express sopra menzionate non fanno parte di z/OS e pertanto l'implementazione delle funzioni crittografiche fornite da tali schede non è stata analizzata.

I test sono stati eseguiti utilizzando tali schede per garantire che le funzioni crittografiche da esse fornite funzionino come previsto. Non è stata eseguita alcuna analisi di vulnerabilità o analisi side-channel per tali funzioni crittografiche. Le affermazioni fatte nel Traguardo di Sicurezza relative alle funzioni crittografiche si applicano solamente alle funzioni implementate dal software o dalla funzione CPACF.

Il sistema operativo z/OS, di cui fa parte l'ODV, può essere eseguito su macchine all'interno di una partizione logica fornita da una versione certificata di IBM PR/SM. Il sistema operativo z/OS può anche essere eseguito su una macchina virtuale fornita da una versione certificata di IBM z/VM.

IBM ha testato individualmente le piattaforme per z/OS (hardware e combinazioni di hardware con IBM PR/SM e/o IBM z/VM) per verificarne la conformità alla z/Architecture utilizzando la suite di test Systems Assurance Kernel (SAK). Questi test assicurano che ogni piattaforma fornisca l'interfaccia di macchina astratta richiesta da z/OS.

Sui sistemi di test è stato eseguito z/OS Version 2 Release 3 nella configurazione certificata. A causa dell'enorme quantità di test, i test sono stati eseguiti durante lo sviluppo dell'ODV. Per garantire che tutti i comportamenti dell'ODV rilevanti per la sicurezza fossero stati testati correttamente, i Valutatori hanno verificato che tutti i test che potrebbero essere stati interessati da qualsiasi modifica rilevante per la sicurezza introdotta alla fine del ciclo di sviluppo fossero stati eseguiti sulla configurazione valutata.

11.2 Test funzionali svolti dal Fornitore

I test RACF sono strettamente integrati nei test del sistema operativo z/OS, che è stato valutato e certificato nello Schema Italiano come OCSI/CERT/ATS/01/2018 [ZOS-RC]. Pertanto, la configurazione per i test di z/OS e il *framework* di test si applicano anche ai test di RACF e possono essere riassunti come segue:

- L'FVT per z/OS viene in gran parte eseguito sul sistema di test VICOM. Si tratta di un sistema z/VM avanzato che implementa l'interfaccia di macchina astratta z/Architecture. Consente ai tester di predisporre singole macchine virtuali di prova che eseguono z/OS con accesso a periferiche virtualizzate come dischi e connessioni di rete. Ai fini dei test delle funzioni di sicurezza, questo ambiente è completamente equivalente alle macchine che eseguono z/OS. Questo ambiente è stato utilizzato anche dai Valutatori per i loro test indipendenti.

- IBM ha fornito un *framework* di test comune per i test che possono essere automatizzati. COMSEC è un ambiente che può essere gestito in modalità standard o in modalità Labeled Security Mode. Il driver di test BERD (Background Environment Random Driver) invia i casi di test come job JES2. L'orientamento di IBM è quello di spostare sempre più test in questo ambiente automatizzato, il che faciliterà sostanzialmente lo sforzo di test richiesto per le valutazioni. A partire dalla versione V1R9 un numero considerevole di test è stato trasferito in questo ambiente. Inoltre, la maggior parte dei team di test ha eseguito i test manuali nell'ambiente di test COMSEC, che fornisce un ambiente di test completo nella configurazione valutata dell'ODV nelle diverse modalità operative.

- Sui sistemi di test è stato eseguito z/OS Version 2 Release 3 nella configurazione certificata. Il team SDF ha fornito un'immagine di sistema preinstallata per VICOM e per le macchine che eseguono i test COMSEC, garantendo così che la versione del software CCEB sia stata utilizzata per tutti i test. I PTF aggiuntivi sono stati applicati ai sistemi VICOM e COMSEC non appena disponibili, con tutti i test rilevanti per la sicurezza per i PTF rieseguiti correttamente. Per alcuni APAR indicati in [TDS] che non sono stati installati sui sistemi di test, un'analisi del loro impatto sulla sicurezza ha rivelato che in realtà non hanno alcun effetto sulle funzionalità dell'ODV sottoposte a test.

11.2.1 Approccio adottato per i test

L'approccio generale ai test di IBM è definito nel processo di Integrated Product Development (IPD) con test dello Sviluppatore, test di verifica funzionale (FVT) e test di verifica del sistema (SVT). Per ogni versione, uno sforzo complessivo di oltre 100 persone viene dedicato a FVT e SVT per i componenti di z/OS, incluso il componente RACF. FVT e SVT vengono eseguiti da team di test indipendenti, con tester diversi dagli sviluppatori. I

diversi team di test hanno sviluppato i propri strumenti di test e per la documentazione di test, ma tutti implementano i requisiti stabiliti nella documentazione di IPD.

Ai fini della valutazione, i test FVT sono di interesse per i Valutatori in quanto comprendono i test per le singole funzioni di sicurezza dichiarate nel Traguardo di Sicurezza [TDS]. IBM ha deciso di creare un *bucket* con i test per le funzioni di sicurezza, riassumendo i test nei singoli piani di test, in modo che i Valutatori avessero la possibilità di gestire la grande mole e complessità dei test di z/OS.

La strategia di test di IBM per la valutazione di z/OS, e quindi di RACF, si è basata su tre fondamenti:

- Nei test di z/OS la principale interfaccia di sicurezza interna è quella con RACF, che è stata testata esaurientemente dal team di test di RACF. Per RACF questi test servono principalmente come test delle interfacce esterne di RACF.
- I componenti che richiedono servizi di Identificazione e Autenticazione o Controllo degli Accessi richiamano RACF (ad eccezione di LDAP LDBM, che implementa il proprio controllo di accesso). Per la maggior parte di questi servizi, è stato sufficiente dimostrare che queste interfacce richiamano RACF, una volta che i test dell'interfaccia di RACF hanno dimostrato il corretto funzionamento interno di RACF.

- A causa della progettazione di z/OS, un gran numero di interfacce interne è visibile anche esternamente, sebbene tali interfacce non siano destinate ad essere richiamate da soggetti esterni non privilegiati. Per queste interfacce, che sono sostanzialmente programmi autorizzati, comandi operatore, determinati servizi richiamabili, routine SVC e PC, i test hanno stabilito unicamente che queste interfacce non possono essere richiamate da soggetti non autorizzati.

A causa della natura dell'ODV e del modo in cui è incorporato in z/OS, non è possibile testarlo in maniera isolata. Ad esempio, una serie di interfacce (i servizi richiamabili di RACF) è destinata a essere utilizzata da USS. Pertanto, alcuni test di USS contribuiscono alla copertura e alla profondità dei test. Questo vale anche per componenti come Binder, CS390, ITDS, BCP, ICSF e JES2. Tali test sono stati considerati per i test RACF in aggiunta ai test originali sul componente RACF.

Tutti i casi di test aggiuntivi e nuovi sono stati progettati in modo da seguire l'approccio dei test già esistenti per il rispettivo componente.

Per i componenti che forniscono funzioni crittografiche, sono stati eseguiti test con e senza il supporto crittografico hardware, al fine di testare il corretto utilizzo delle funzioni crittografiche hardware, se presenti, e la corretta implementazione software all'interno dell'ODV.

11.2.2 Copertura dei test

Lo Sviluppatore ha fornito una mappatura tra il TSF descritto nel Traguardo di Sicurezza [TDS], le TSFI indicate nelle specifiche funzionali e i test eseguiti. I Valutatori hanno verificato questa mappatura ed esaminato i casi di test per verificare che i test coprissero le funzioni di sicurezza e le loro interfacce. Sebbene non siano richiesti test approfonditi, il

Committente ha fornito prove del fatto che sono stati sottoposti a test dettagli significativi delle funzioni di sicurezza.

I Valutatori hanno stabilito che i test dello Sviluppatore hanno fornito la copertura richiesta. I test hanno riguardato l'intero TSF descritto nel Traguardo di Sicurezza e tutte le interfacce identificate nelle specifiche funzionali.

La profondità dei test è stata verificata rispetto ai sottosistemi dell'ODV ed ai moduli che realizzano le funzioni di sicurezza. Per la maggior parte delle funzioni di sicurezza rilevanti per questa valutazione, i sottosistemi invocano le funzioni di RACF per prendere decisioni rilevanti per la sicurezza; il controllo degli accessi, l'identificazione e l'autenticazione, la gestione della sicurezza e la generazione dei record di audit rilevanti per la sicurezza sono per lo più gestiti da RACF. Tutte le altre funzioni rilevanti per la sicurezza sono implementate all'interno dei sottosistemi stessi, mantenendo così isolate le funzioni di sicurezza al loro interno. Per l'autoprotezione, BCP e la macchina astratta sottostante lavorano insieme per fornire protezione della memoria e diversi meccanismi di autorizzazione come APF o AKM.

I Valutatori hanno verificato che tutti i dettagli rilevanti per la sicurezza del progetto dell'ODV a livello di sottosistemi sono stati presi in considerazione per i test. In particolare, il test delle interfacce del sottosistema RACF è stato eseguito direttamente su queste interfacce, oltre che sui sottosistemi che invocano RACF.

11.2.3 Risultati dei test

I risultati dei test forniti dal Committente sono stati generati sulle configurazioni descritte in precedenza. Sebbene diversi team di test abbiano utilizzato strumenti e database di tracciamento dei test diversi, i Valutatori hanno verificato che tutti i risultati forniti mostravano che i test erano stati eseguiti correttamente e avevano prodotto i risultati previsti.

I test effettuati sono risultati validi sia per la modalità operativa standard, sia per la modalità Labeled Security Mode, ad eccezione dei test per le funzionalità di sicurezza multilivello, rilevanti solo per la modalità Labeled Security Mode. I sistemi di test configurati per la modalità Labeled Security Mode sono conformi anche alla modalità standard, quindi i test eseguiti su questi sistemi sono sempre applicabili a entrambe le modalità operative. Per COMSEC, tutti i test applicabili sono stati eseguiti in configurazioni dedicate in modalità Labeled Security Mode e in modalità standard.

I Valutatori hanno verificato che i test sono stati eseguiti su configurazioni conformi al Traguardo di Sicurezza [TDS]. I Valutatori sono stati in grado di seguire e comprendere appieno l'approccio ai test sulla base delle informazioni fornite dallo Sviluppatore. Tramite questo ambiente di test, lo Sviluppatore è stato in grado di fornire ai Valutatori la prova della necessaria copertura e profondità dei test.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

I test indipendenti dei Valutatori hanno seguito la guida [CEM] per verificare ogni funzione di sicurezza, senza ripetere in maniera esaustiva tutti i test dello Sviluppatore. I Valutatori hanno deciso di concentrarsi sulle principali funzioni di sicurezza dell'ODV al fine di fornire una verifica indipendente del loro corretto funzionamento:

- Identificazione e autenticazione: i Valutatori hanno predisposto solo alcuni test di base, per lo più impliciti, delle funzioni di identificazione e autenticazione in TSO/E, ftp, su e JES, in quanto queste funzioni sono state sollecitate ampiamente durante l'attività dei tester. Tali test si sono concentrati sui meccanismi di autenticazione basati su Kerberos.

- Controllo di accesso discrezionale (DAC): i Valutatori si sono concentrati sulle ACL degli UNIX System Services, testando implicitamente anche i bit di permessi di UNIX. Altri test sul DAC hanno riguardato:

    - USS IPC (tutte le chiamate di sistema per messaggi, semafori e memoria condivisa);

    - DAC per diversi oggetti USS (file speciali di dispositivi, oggetti IPC, directory);

    - accesso ai set di dati di z/OS;

    - chiamate di sistema di USS rilevanti per la sicurezza che si interfacciano internamente con RACF.

- Controllo di accesso vincolato (MAC): i Valutatori hanno rieseguito come test di regressione i propri test sui controlli MAC per set di dati e file di UNIX System Services. È stato inoltre eseguito il test della capacità di modifica del privilegio di *write-down* dei profili di classe FACILITY.

- Funzionalità di audit: sono stati eseguiti test per verificare l'audit delle modifiche all'orologio di sistema.

- Gestione della sicurezza: i Valutatori hanno deciso di non predisporre test speciali per questo aspetto, dal momento che la configurazione dell'ambiente di test e il *setup/cleanup* dei test includono già una parte importante di questa parte del TSF.

- Autoprotezione dell'ODV: l'unico aspetto a poter essere adeguatamente verificabile è il riutilizzo degli oggetti, riguardo il quale i Valutatori hanno deciso di concentrarsi sul problema delle pagine di memoria che potrebbero contenere informazioni residue.

Affinché la serie di test degli Sviluppatori potesse essere rieseguita e osservata, i Valutatori hanno scelto un approccio integrativo per i test e si sono concentrati sulle funzionalità modificate rispetto alla valutazione precedente.

I Valutatori hanno deciso di concentrarsi sulle funzioni di sicurezza dichiarate nel Traguardo di Sicurezza [TDS] e di non eseguire test tesi a dimostrare che le funzioni che richiedono l'autorizzazione falliscono se invocate senza privilegi. Ciò è stato in parte dovuto al fatto che i Valutatori avevano già avuto sufficienti riscontri della protezione delle funzioni di sicurezza durante la predisposizione del sistema nella sua configurazione valutata, seguendo le indicazioni in [MLSGUIDE].

Oltre ad aver rieseguito un campione dei test dello Sviluppatore ed osservato l'esecuzione dei test da parte dei tester IBM durante sessioni dedicate, i Valutatori hanno acquisito evidenza dell'impegno dello Sviluppatore durante la loro lunga permanenza nel sito di

sviluppo. In tale contesto, i Valutatori hanno discusso con i tester problemi riscontrati o interpretazioni dei requisiti CC e hanno assistito all'esecuzione dei test durante la creazione del *bucket* dei test. I Valutatori avevano già intervistato i tester durante le visite ispettive ed esaminato i database con i casi di test ed i relativi risultati e record di esecuzione.

Tutti i test sono stati eseguiti sul sistema di test VICOM, configurato dai Valutatori in base alle specifiche della guida [MLSGUIDE], e sul sistema COMSEC predisposto da IBM e verificato dai Valutatori essere nella configurazione valutata. Un'eccezione a questo approccio ha riguardato le *patch* aggiuntive, raccomandate dallo Sviluppatore per l'ODV, anche se non facevano parte della configurazione CC per i test. I Valutatori hanno esaminato le informazioni su queste *patch* fornite dallo Sviluppatore e hanno stabilito che non influiscono sul comportamento delle funzioni di sicurezza da sottoposte a test.

Durante le loro sessioni di test i Valutatori hanno potuto verificare che tutte le funzionalità sottoposte a test hanno mostrato il comportamento atteso.

11.4 Analisi delle vulnerabilità e test di intrusione

Per quanto riguarda l'analisi delle vulnerabilità, le modifiche introdotte in RACF V2R3 rispetto alla versione precedente dell'ODV non hanno fornito molte aree di interesse per i test di intrusione.

I test di intrusione dei Valutatori hanno riguardato il seguente aspetto, non coperto nelle precedenti valutazioni:

- Le chiamate di sistema di USS come *front-end* per i servizi di RACF.

I test di intrusione hanno stimolato le chiamate di sistema disponibili, fornendo argomenti casuali. Nessuna funzione di sicurezza specifica è stata sottoposta a test. Tuttavia, le chiamate di sistema rappresentano l'intero insieme di funzioni disponibili per i soggetti USS.

Qualsiasi problema che si fosse verificato durante il test di una chiamata di sistema, avrebbe potenzialmente avuto un impatto negativo sulle funzioni di sicurezza invocate da quella chiamata di sistema. I test hanno riguardato sia il sottosistema USS, sia RACF.

Poiché l'ODV ha resistito a tutti i test di penetrazione effettuati, i Valutatori hanno potuto concludere che nessuno scenario di attacco con potenziale Moderate o inferiore può essere portato a termine con successo nell'ambiente operativo dell'ODV nel suo insieme. Non sono state identificate vulnerabilità residue.