Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

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. 1/22

(Certification No.)

Prodotto: IBM z/OS Version 2 Release 4

(Product)

Sviluppato da: IBM Corporation

(Developed by)

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

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

EAL4+
(ALC_FLR.3)

Il Direttore
(Dott.ssa Eva Spina)

Firmato digitalmente
da Eva Spina
Data: 2022.01.13
13:09:50 +01'00'

Roma, 13 gennaio 2022

Fino a EAL2 *(Up to EAL2)*

Questa pagina è lasciata intenzionalmente vuota

Organismo di Certificazione della Sicurezza Informatica

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

IBM z/OS Version 2 Release 4

OCSI/CERT/ATS/03/2020/RC

Versione 1.0

13 gennaio 2022

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	13/01/2022

2 Indice

3 Elenco degli acronimi

ABEND	Abnormal End
AES	Advanced Encryption Standard
AKM	Access Key Mask
APAR	Authorized Program Analysis Report
APF	Authorized Program Facility
API	Application Programming Interface
APPC/MVS	Advanced Program-to-Program Communication / Multiple Virtual Storage
AT-TLS	Application Transparent Transport Layer Security
BCP	Base Control Program
BDT	Bulk Data Transfer
BERD	Background Environment Random Driver
BSC	Binary Synchronous Communication
CA	Certificate Authority
CC	Common Criteria
CCEB	Common Criteria Evaluated Base
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CPACF	Central Processor Assist for Cryptographic Function
CVE	Common Vulnerabilities and Exposures
DES	Data Encryption Standard
DFS	Distributed File Service
DFSMS	Data Facility Storage Management Subsystem
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
EIM	Enterprise Identity Mapping

FTP	File Transfer Protocol
FVT	Functional Verification Tests
HASP	Houston Automatic Spooling Priority
HMAC	Keyed-hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
ICSF	Integrated Cryptographic Service Facility
ID	Identifier
IKE	Internet Key Exchange
IP	Internet Protocol
IPD	Integrated Product Development
IPL	Initial Program Load
IPSec	IP Security
IT	Information Technology
JES	Job Entry System
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
NJE	Network Job Entry
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
OS	Operating System
PC	Program Call
PKCS	Public-Key Cryptography Standards
PP	Profilo di Protezione (Protection Profile)
PR/SM	Processor Resource/System Manager
PTF	Program Temporary Fix

RACF	Resource Access Control Facility
RFC	Request for Comments
RFV	Rapporto Finale di Valutazione
RRSF	RACF Remote Sharing Facility
SAK	System Assurance Kernel
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SMB	Server Message Block
SMF	System Management Facilities
SNA	Systems Network Architecture
SHA	Secure Hash Algorithm
SSH	Secure SHell
ST	Security Target
SVC	Supervisor Call
SVT	System Verification Tests
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol
TDES	Triple DES
TDS	Traguardo di Sicurezza
TLS	Transport Layer Security
TOE	Target Of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSO	Time Sharing Option
TSO/E	TSO Extensions
UID	User Identifier
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

[GPOSPP] Protection Profile for General Purpose Operating Systems, NIAP, Version 4.2.1, 22 April 2019

[MLSGUIDE] “z/OS V2.4 - Planning for Multilevel Security and the Common Criteria”, GA32-0891-40, 23 May 2021

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

[OSPP-EIA] OSPP Extended Package – Extended Identification and Authentication, Version 2.0, BSI-CC-PP-0067, 28 May 2010

[OSPP-LS] OSPP Extended Package – Labeled Security, Version 2.0, BSI-CC-PP-0067, 28 May 2010

[RC] Rapporto di certificazione “IBM z/OS Version 2 Release 3”, OCSI/CERT/ATS/01/2018/RC, versione 1.0, 31 luglio 2019

[RFVv1] Final Evaluation Technical Report “IBM z/OS Version 2 Release 4”, Version 1, atsec information security GmbH, 20 October 2021

[RFVv2] Final Evaluation Technical Report “IBM z/OS Version 2 Release 4”, Version 2, atsec information security GmbH, 10 January 2022

[TDS] “IBM z/OS Version 2 Release 4 Security Target”, Version 1.3, IBM Corporation, 10 January 2022

[ZARCH] “z/Architecture Principles of Operation”, SA22-7832-12, September 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 EAL2, 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 https://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 z/OS Version 2 Release 4", sviluppato da International Business Machines Corp. (IBM), nel seguito del documento anche indicato come z/OS V2R4 o z/OS.

L'ODV è un sistema operativo *general-purpose*, multiutente e multitasking per sistemi informatici aziendali.

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).

Il presente Rapporto di Certificazione è stato emesso a conclusione della ri-certificazione di una precedente versione dello stesso ODV (IBM z/OS Version 2 Release 3), già certificato dall'OCSI (Certificato n. 6/19 del 31 luglio 2019 [RC]).

In seguito ad alcune modifiche apportate al prodotto da parte del Fornitore IBM Corp. è stato necessario procedere a una ri-certificazione dell'ODV. In particolare, una serie di funzioni e servizi di sicurezza dell'ODV V2R3 non sono più compresi nell'ambito dell'ODV V2R4. Inoltre, la nuova versione dell'ODV V2R4 non dichiara più la conformità a [OSPP] e ai relativi pacchetti estesi ([OSPP-EIA], [OSPP-LS]) o ad altri PP. Tuttavia, l'LVS atsec information security GmbH ha potuto riutilizzare parte della documentazione e delle evidenze già fornite nella precedente valutazione.

Si noti che le modifiche effettuate hanno comportato anche la revisione del Traguardo di Sicurezza [TDS]. Gli utenti della precedente versione dell'ODV sono quindi invitati a prendere visione anche del nuovo TDS.

Pur rimanendo valide in gran parte le considerazioni e le raccomandazioni già espresse per il precedente ODV, per facilità di lettura il presente Rapporto di Certificazione è stato riscritto nella sua interezza in modo da costituire un documento autonomo associato al nuovo ODV "IBM z/OS Version 2 Release 4".

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 e/o utilizzatori. 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 EAL4, con l'aggiunta di ALC_FLR.3, in conformità a quanto riportato 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 specifica l'esito della valutazione di sicurezza del prodotto "IBM z/OS Version 2 Release 4" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti e/o utilizzatori per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

Il presente Rapporto di Certificazione deve essere consultato 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 z/OS Version 2 Release 4
Traguardo di Sicurezza	IBM z/OS Version 2 Release 4 Security Target, Version 1.3 [TDS]
Livello di garanzia	EAL4 con l'aggiunta di ALC_FLR.3
Fornitore	IBM Corporation
Committente	IBM Corporation
LVS	atsec information security GmbH
Conformità a PP	3.1 Rev. 5
PP conformance claim	Nessuna conformità dichiarata
Data di inizio della valutazione	21 maggio 2020
Data di fine della valutazione	20 ottobre 2021

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 paragrafo 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 software z/OS Versione 2 Release 4 (V2R4), inclusa la documentazione di accompagnamento e gli APAR SW come dettagliato in Tabella 2.

z/OS è un sistema operativo *general-purpose*, multiutente e multitasking per i sistemi informatici aziendali. Più utenti possono utilizzare z/OS contemporaneamente per eseguire

una varietà di funzioni che richiedono un accesso controllato e condiviso alle informazioni memorizzate nel sistema.

Per una descrizione dettagliata dell'ODV, si consulti il par. 1.5 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito.

7.3.1 Architettura dell'ODV

7.3.1.1 Panoramica generale dell'ODV

L'ODV è il sistema operativo z/OS con i componenti software elencati in Tabella 2.

L'ODV è un'istanza di z/OS in esecuzione su una macchina astratta come unico sistema operativo e che esercita il pieno controllo su questa macchina astratta. La macchina astratta, la maggior parte della quale non fa parte dell'ODV come descritto di seguito, può essere fornita da:

- una partizione logica fornita da una versione certificata di PR/SM in esecuzione su IBM z15 con CPACF DES/TDES Enablement Feature 3863 attivo, con schede Crypto Express7S;

- una versione certificata di IBM z/VM® in esecuzione in una partizione logica fornita da PR/SM su processori System z™.

La maggior parte della macchina astratta non fa parte dell'ODV, ma appartiene all'ambiente operativo dell'ODV. Tuttavia, la correttezza dei meccanismi di separazione e protezione della memoria implementati nella macchina astratta è stata analizzata nell'ambito della valutazione in quanto tali funzioni sono cruciali per la sicurezza dell'ODV.

Singole istanze dell'ODV possono essere eseguite da soli o all'interno di una rete come un insieme di *host* cooperanti, che implementano lo stesso insieme di politiche di sicurezza ed operano in accordo ad esso. Questi *host* possono anche essere connessi per formare un complesso di sistemi a basso grado di accoppiamento chiamato *sysplex*.

La maggior parte delle funzioni di sicurezza dell'ODV (TSF) sono fornite dai componenti del sistema operativo z/OS Base Control Program (BCP) e Resource Access Control Facility (RACF). Quest'ultimo componente di z/OS è utilizzato da diversi servizi come istanza centrale per l'identificazione e l'autenticazione e per le decisioni di controllo degli accessi. z/OS è dotato di funzioni di gestione che consentono di configurare le funzioni di sicurezza dell'ODV per adattarle alle esigenze dell'utilizzatore.

Nell'ODV sono stati inseriti alcuni elementi che non forniscono funzioni di sicurezza. Questi elementi funzionano in modalità autorizzata e possono quindi compromettere l'ODV se non si comportano correttamente. Poiché questi elementi sono essenziali per il funzionamento di molti ambienti dei clienti, la loro inclusione richiede che siano sottoposti durante la valutazione ad un processo di verifica che garantisca che possano essere utilizzati dai clienti senza influire sulla sicurezza dell'ODV.

7.3.1.2 Principali componenti software dell'ODV

z/OS Version 2 Release 4 include i seguenti principali sottosistemi:

- **Base Control Program (BCP)**: BCP è il sottosistema principale di z/OS, responsabile della gestione dell'archiviazione (reale e virtuale), della gestione degli spazi degli indirizzi, delle attività e degli SRB, della pianificazione, della gestione di interruzioni ed eccezioni, della sincronizzazione e di altri servizi di base.

- **System Management Facilities (SMF)**: SMF raccoglie e registra le informazioni relative al sistema e ai job che l'installazione può utilizzare per: controllo degli utenti, affidabilità dei report, analisi della configurazione, pianificazione dei job, riepilogo dell'attività dei volumi ad accesso diretto, valutazione dell'attività del set di dati, profilazione dell'utilizzo delle risorse di sistema, mantenimento della sicurezza del sistema.

- **Data Facility Storage Management Subsystem (DFSMS)**: l'archiviazione gestita dal sistema è l'approccio automatizzato IBM alla gestione delle risorse di archiviazione. Utilizza programmi software per gestire la sicurezza, il posizionamento, la migrazione, il backup, il richiamo, il ripristino e la cancellazione dei dati in modo che i dati correnti siano disponibili quando necessario, lo spazio sia reso disponibile per la creazione di nuovi dati e per l'estensione dei dati correnti e i dati obsoleti vengano rimossi dallo spazio di archiviazione.

- **Resource Access Control Facility (RACF)**: RACF è il componente centrale di z/OS responsabile dell'identificazione e dell'autenticazione degli utenti, del controllo di accesso e della generazione di record di audit relativi agli eventi di sicurezza (che RACF invia a SMF per fare in modo che i record di audit siano inclusi nell'audit di SMF).

- **Integrated Cryptographic Service Facility (ICSF)**: ICSF è il principale fornitore di servizi crittografici di base di z/OS e per le funzioni specificate negli SFR. Viene utilizzato per i servizi crittografici di base per la generazione di certificati/chiavi, per i certificati utilizzati per l'autenticazione degli utenti, nonché per i certificati utilizzati nella creazione di canali attendibili.

- **Communications Server**: Il componente Communications Server di z/OS è responsabile dell'implementazione dello *stack* TCP/IP e dei protocolli di livello superiore (tranne SSH). Come funzionalità di sicurezza il Communications Server fornisce: controllo dell'accesso agli oggetti, canali attendibili, funzionalità di *IP filtering*.

- **Job Entry Subsystem 2 (JES2)**: z/OS utilizza un sottosistema di immissione dei job (JES) per ricevere i job nel sistema operativo, pianificarli per l'elaborazione da parte di z/OS e per controllare l'elaborazione dell'output. JES2 discende da HASP (Houston Automatic Spooling Ppriority). HASP è definito come un programma per computer che fornisce funzioni supplementari per la gestione dei job, la gestione dei dati e le attività come la pianificazione, il controllo del flusso dei job e lo spooling.

- **Time Sharing Option (TSO/E)**: TSO/E è l'interfaccia utente principale del sistema z/OS. TSO/E fornisce numerosi comandi sia per gli utenti finali, sia per i programmatori di sistema, che consentono loro di interagire con TSO/E e il sistema z/OS.

- **UNIX System Services (USS)**: Il supporto di z/OS per z/OS UNIX abilita due interfacce di sistemi aperti sul sistema operativo z/OS: un'API (Application Programming Interface) conforme a XPG4 UNIX 1995 e un'interfaccia interattiva di *shell* per z/OS.

- **OpenSSH**: Secure Shell (SSH) è un protocollo di rete che fornisce un'alternativa per l'accesso remoto non sicuro e funzionalità di esecuzione dei comandi, come `telnet`, `rlogin` e `rsh`. SSH cifra il traffico in entrambe le direzioni, prevenendo lo sniffing e il furto di password. L'SSH fornito per z/OS è un *port* di OpenSSH 6.4p1, disponibile su www.openssh.org.

7.3.2 Caratteristiche di sicurezza dell'ODV

7.3.2.1 Politica di sicurezza dell'ODV

Le principali caratteristiche di sicurezza dell'ODV sono:

- identificazione e autenticazione;
- controllo discrezionale degli accessi;
- auditing;
- riutilizzo degli oggetti;
- gestione della sicurezza;
- comunicazione sicura;
- protezione del TSF;
- protezione della riservatezza dei set di dati.

Queste funzionalità sono supportate dalla separazione dei domini e dalla mediazione dei riferimenti, che assicurano che siano sempre richiamate e non possano essere aggirate.

7.3.2.2 Obiettivi di sicurezza dell'ambiente operativo

Le ipotesi per il corretto funzionamento dell'ODV sono definite nel par. 3.3 del Traguardo di Sicurezza [TDS]. I seguenti obiettivi per l'ambiente operativo vanno in particolare assicurati:

- Il sistema operativo è installato su hardware affidabile.
- L'utente del sistema operativo non è intenzionalmente negligente o ostile e utilizza il software in conformità con la politica di sicurezza aziendale applicata. Gli account utente standard vengono forniti in base al modello con privilegi minimi. Gli utenti che richiedono livelli di accesso più elevati dovrebbero avere un account separato dedicato a tale uso.

- L'amministratore del sistema operativo non è incurante, intenzionalmente negligente o ostile e amministra il sistema operativo nel rispetto della politica di sicurezza aziendale applicata.

- Se l'ODV fa affidamento su sistemi IT remoti attendibili per supportare l'applicazione della propria policy, tali sistemi forniscono le funzioni richieste dall'ODV e sono sufficientemente protetti da qualsiasi attacco che potrebbe causare la restituzione di risultati falsati da parte di tali funzioni.

- 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 potrebbero compromettere gli obiettivi di sicurezza IT. La protezione deve essere commisurata al valore degli *asset* informatici tutelati dall'ODV.

- I responsabili dell'ODV devono garantire che siano fornite procedure e/o meccanismi per assicurare che, dopo un guasto del sistema o altra discontinuità, questo venga ripristinato senza compromissione della protezione (sicurezza).

- I sistemi IT remoti attendibili implementano i protocolli ei meccanismi richiesti dal TSF per supportare l'applicazione della politica di sicurezza.

Per una descrizione completa degli obiettivi di sicurezza per l'ambiente operativo dell'ODV, si consulti il par. 4.2 del Traguardo di Sicurezza [TDS].

7.3.2.3 Funzioni di sicurezza

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consulti il capitolo 7 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito:

- **Identificazione e Autenticazione**: z/OS fornisce vari metodi per l'identificazione ed autenticazione degli utenti.

- **Controllo di Accesso Discrezionale (DAC)**: z/OS supporta controlli di accesso che sono in grado di imporre limitazioni su singoli utenti e *data object*; RACF attua le decisioni sul controllo di accesso basandosi sull'identità degli utenti, sugli attributi di sicurezza, sulle autorità di gruppo e sulle autorizzazioni di accesso specificate nel profilo delle risorse.

- **Sicurezza delle comunicazioni**: z/OS fornisce diverse modalità di comunicazione sicura tra sistemi che condividono la stessa politica di sicurezza, inclusi i canali di comunicazione attendibili per le connessioni TCP/IP, supporta il protocollo SSH v2, il protocollo IP Security (IPSec) con Internet Key Exchange (IKE).

- **Gestione della sicurezza**: z/OS fornisce un insieme di comandi e di opzioni per gestire adeguatamente le funzioni di sicurezza dell'ODV; inoltre, l'ODV fornisce la funzionalità di gestione degli utenti, di gruppi di utenti e di profili generali per le risorse.

- **Funzionalità di Audit**: l'ODV fornisce una funzionalità di audit che permette di generare record di audit per eventi critici per la sicurezza; RACF fornisce alcune

funzioni di log e di reportistica che permettono ai proprietari delle risorse e agli auditor di identificare gli utenti che tentano di accedere alle risorse.

- **Riuso degli oggetti**: il riuso degli oggetti protetti e l'archiviazione è gestito da vari controlli hardware e software, e da procedure amministrative.

- **Protezione del TSF**: la protezione del TSF è basata su numerosi meccanismi di protezione che sono supportati dalle macchine astratte sottostanti su cui z/OS è in esecuzione.

- **Protezione della confidenzialità dei set di dati**: con la protezione della riservatezza dei set di dati di z/OS, gli utenti possono cifrare i dati a piacimento senza che siano richiesti cambiamenti di applicazioni.

7.3.3 Funzioni crittografiche

Le funzioni crittografiche implementate dai coprocessori CEX7S fanno parte dell'ambiente operativo dell'ODV e pertanto non sono state valutate con l'estensione richiesta dal livello di garanzia previsto. Si noti che un coprocessore crittografico è necessario per l'operatività dell'ODV nella sua configurazione valutata.

Un utente che desidera utilizzare le funzioni crittografiche fornite da un coprocessore deve essere consapevole del fatto che, sebbene tali funzioni crittografiche siano state testate durante la valutazione rispetto alla correttezza funzionale, non è stata eseguita alcuna ulteriore analisi della progettazione e dell'implementazione di tali funzioni. In particolare non è stata eseguita alcuna verifica della presenza di *side channel* potenzialmente sfruttabili nell'implementazione delle funzioni crittografiche fornite dai coprocessori.

Le dichiarazioni fatte nel Traguardo di Sicurezza in merito alle funzioni crittografiche si applicano quindi alle funzioni implementate nel software o da CPACF.

Le funzioni crittografiche sono descritte con maggiore dettaglio nel par. 6.1.2 del Traguardo di Sicurezza [TDS]. Il par. 5.1 definisce anche i componenti estesi per il supporto crittografico.

7.4 Documentazione

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

Devono inoltre essere seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel par. 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].

Tutti i Requisiti Funzionali di Sicurezza (SFR) sono stati selezionati o derivati per estensione dai CC Parte 2 [CC2].

Tutti i requisiti estesi definiti nel Traguardo di Sicurezza [TDS] sono stati tratti dal PP [GPOSPP], sebbene il TDS non dichiari conformità a questo PP. Gli SFR derivati da [GPOSPP] sono distinguibili dagli SFR selezionati dai CC Parte 2 dal suffisso "_EXT" o dall'aggiunta del termine "(Refined)".

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, gli 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 20 ottobre 2021 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFVv1]. Una versione aggiornata dell'RFV [RFVv2] contenente solo modifiche di lieve entità è stata approvata dall'Organismo di Certificazione il 12 gennaio 2022. 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 ([RFVv1] e [RFVv2]) 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 z/OS Version 2 Release 4" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, con 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 EAL4, con 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 functional specification	ADV_FSP.4	Positivo
Implementation representation of the TSF	ADV_IMP.1	Positivo
Basic modular design	ADV_TDS.3	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
Problem tracking CM coverage	ALC_CMS.4	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
Well-defined development tools	ALC_TAT.1	Positivo
Systematic flaw remediation	*ALC_FLR.3*	Positivo
Tests	**Classe ATE**	Positivo
Analysis of coverage	ATE_COV.2	Positivo
Testing: basic design	ATE_DPT.1	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing – sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Focused vulnerability analysis	AVA_VAN.3	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 z/OS Version 2 Release 4" 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 agli Obiettivi di Sicurezza per l'ambiente operativo specificati nel cap. 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 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]).

Si assume che l'ODV funzioni in modo sicuro qualora vengano rispettate le ipotesi sull'ambiente operativo descritte nel par. 3.3 del documento [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 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 documento [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

La versione valutata di z/OS può essere ordinata tramite un rappresentante di vendita IBM o tramite l'applicazione Web ShopzSeries (http://www.ibm.com/software/shopzseries). Quando s'inoltra un ordine tramite servizi Internet (protetti), IBM richiede ai clienti il possesso di un account con un nome di login e una password. La registrazione per tale account a sua volta richiede un ID cliente valido fornito da IBM.

In Tabella 2 sono elencati gli elementi che costituiscono l'ODV, inclusi il software e la documentazione di guida.

#	Tipo	Identificativo	Release	Metodo di consegna
z/OS Version 2 Release 4 (z/OS V2.4, program number[1] 5650-ZOS) Common Criteria Evaluated Base Package				
1	SW	z/OS V2.4 Common Criteria Evaluated Base (IBM program number 5650-ZOS)	V2R4	Nastro
2	DOC	z/OS V2.4 Program Directory	GI11-9848-03	Copia cartacea
3	DOC	z/OS V2R4 Library V2R4 Nome file di archivio: zOSV2R4Library.zip	V2R4	Copia elettronica
		Da scaricare da: https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R4Library Selezionare "Download all z/OS V2R4 Library publications to ZIP file"		
4	DOC	ServerPac: IYO (Installing Your Order)	n/d	Copia cartacea
5	DOC	Memo to Customers of z/OS V2.4 Common Criteria Evaluated Base	n/d	Copia cartacea
6	DOC	z/OS V2.4 Planning for Multilevel Security and the Common Criteria Nome del file: e0ze100_v2r4.pdf Ultimo aggiornamento: 23-05-2021 SHA256 checksum: 65cd99fb8f96d18ea6b2f2a7e7d2a4dae6b4c8c39cf615908cda4d1bf9f8c3ba	GA32-0891-40	Copia elettronica
Elementi aggiuntivi				
7	SW	PTFs per i seguenti APAR (necessari): • OA57641 (PTF UJ02099) • OA57934 (PTF UJ00393) • OA58067 (PTF UJ02223) • OA58074 (PTF UJ02931) • OA58282 (PTF UJ01931) • OA58313 (PTF UJ02442)	n/d	Copia elettronica

[1] Il "program number" (o "product number") è l'identificazione tecnica di IBM per il prodotto "z/OS". Viene utilizzato per scopi di ordine e licenza e non identifica in modo univoco l'ODV. La stringa "z/OS Version 2 Release 4" identifica in modo univoco l'ODV.

#	Tipo	Identificativo	Release	Metodo di consegna
		• OA58349 (PTF UJ02614) • OA58505 (PTF UJ01875) • OA58588 (PTF UJ01732) • OA58595 (PTF UJ01957) • OA58781 (PTF UJ01929 & PTF UJ01933) • OA58990 (PTF UJ02368 & PTF UJ02370) • OA59021 (PTF UJ02052) • OA59040 (PTF UJ02630) • OA59074 (PTF UJ02508 & PTF UJ02509) • OA59156 (PTF UJ02505) • OA59268 (PTF UJ02741 & PTF UJ02741) • PH14146 (PTF UI68531) • PH14509 (PTF UI66980) • PH14511 (PTF UI67180) Queste PTF debbono essere ottenute in formato elettronico da ShopzSeries (https://www.ibm.com/software/shopzseries)		

Tabella 2 – Elementi consegnabili dell'ODV

La consegna di tutti gli elementi avviene in un unico pacchetto, prodotto appositamente per gli acquirenti e spedito tramite corriere. Gli aggiornamenti aggiuntivi devono essere scaricati successivamente dall'acquirente dal sito Web ShopzSeries, seguendo le istruzioni fornite con il pacchetto.

La distribuzione elettronica delle guide avviene tramite il sito Web IBM all'indirizzo https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R4Library. Gli utenti possono scaricare l'intero pacchetto della documentazione di guida dell'ODV (elemento 3 in Tabella 2) facendo clic sul collegamento "Download all z/OS V2R4 Library publications to ZIP file". Il download è protetto dal protocollo HTTPS, che può essere verificato dagli utenti facendo clic sul simbolo del lucchetto nel campo dell'indirizzo del proprio browser per visualizzare il certificato IBM. L'archivio ZIP risultante, denominato zOSV2R4Library.zip, contiene anche il documento [MLSGUIDE] (elemento 6 in Tabella 2), che contiene ulteriori istruzioni su come impostare l'ODV nella sua configurazione valutata.

9.2 Identificazione dell'ODV

Gli elementi consegnati al cliente sono etichettati con i numeri di prodotto, di documento e di versione come indicato nella Tabella 2 e possono essere verificati dagli utenti che installano il sistema.

Il riferimento all'ODV può essere verificato dall'amministratore durante il caricamento iniziale del programma (IPL), quando viene visualizzata sulla console di sistema l'identificazione del sistema. Per visualizzare la versione di z/OS, l'operatore può anche impartire il comando `D IPLINFO`. La stringa "z/OS 02.04.00" dovrebbe essere visualizzata tra le altre informazioni.

9.3 Installazione, inizializzazione e utilizzo sicuro dell'ODV

9.3.1 Installazione e configurazione del software

L'Oggetto della Valutazione (ODV) è il prodotto "z/OS Version 2 Release 4" sviluppato dalla società IBM Corporation. L'ODV è composto unicamente da software ed è accompagnato dalla documentazione di guida. Gli elementi elencati in Tabella 2 rappresentano l'ODV.

Il pacchetto z/OS V2R4 Common Criteria Evaluated Base deve essere installato seguendo le istruzioni fornite con il supporto e configurato secondo le istruzioni nel capitolo 7 del documento [MLSGUIDE]. Inoltre, devono essere installate tutte le PTF richieste elencate come elemento 7 in Tabella 2.

Durante l'installazione è possibile scegliere di non utilizzare nessuno degli elementi forniti all'interno del ServerPac, ma è comunque richiesta l'installazione, la configurazione e l'utilizzo del componente RACF dell'elemento z/OS Security Server.

Inoltre, qualsiasi software non facente parte dell'ODV può essere aggiunto senza compromettere le caratteristiche di sicurezza del sistema, a patto che non possa essere eseguito:

- nello stato supervisor;
- come *APF-authorized*:
- con chiavi da 0 a 7;
- con UID(0);
- con autorità a risorse FACILITY quali BPX.DAEMON, BPX.SERVER, o BPX.SUPERUSER;
- con autorità a risorse UNIXPRIV.

Questo esclude esplicitamente:

- sostituzione di qualsiasi elemento nel ServerPac che fornisce funzioni di sicurezza rilevanti per questa valutazione con altri prodotti di terze parti;
- installazione di *system exit* che sono in esecuzione autorizzata (stato supervisor, *system key*, o *APF-authorized*), con l'eccezione dell'elemento ICHPWX11 e della sua routine associata IRRPHREX;
- utilizzo della Authorized Caller Table (ICHAUTAB) in RACF per permettere a programmi non autorizzati di emettere RACROUTE REQUEST=VERIFY (RACINIT) o RACROUTE REQUEST=LIST (RACLIST).

Nota: la configurazione valutata del software non è invalidata dall'installazione e dal funzionamento di altri componenti opportunamente certificati che possono essere eseguiti in modalità autorizzata. Tuttavia, la valutazione di tali componenti deve dimostrare che il

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

Il demone SSH `sshd` può essere utilizzato a condizione che:

- sia configurato per l'utilizzo del protocollo 2 e di una *suite* di cifratura basata su AES,
- sia configurato modalità di separazione dei privilegi, e
- sia configurato per permettere unicamente l'autenticazione degli utenti basata su password (o *passphrase*) o basata su chiave pubblica con le chiavi pubbliche immagazzinate nei *keyring* di RACF. Autenticazione di utente basata su Rhost o su chiave pubblica con chiavi immagazzinate altrove non è consentita nella configurazione valutata.

TLS:

- Se utilizzato, TLS (Transport Layer Security) deve usare i protocolli TLS V1.2 o TLS V1.3. TLS deve inoltre utilizzare una delle *suite* di cifratura elencate nell'SFR FCS_TLSC_PLUS.1 del Traguardo di Sicurezza [TDS].
- Qualsiasi applicazione che esegue l'autenticazione del client mediante certificati digitali client su TLS deve essere configurata per utilizzare i profili RACF nelle classi RACDCERT o DIGTRING o i *token* PKCS#11 in ICSF per archiviare i *keyring* che contengono la chiave privata dell'applicazione ed i certificati consentiti dell'autorità di certificazione (CA) che possono essere utilizzati per fornire i certificati client che l'applicazione supporterà. L'uso di `gskkyman` per questo scopo non fa parte della configurazione valutata.

Communications Server:

- Il server e il client FTP di z/OS e il server TN3270 di z/OS supportano sia TLS configurato manualmente, sia AT-TLS. Questa valutazione ha preso in considerazione solo le configurazioni AT-TLS e, di conseguenza, la configurazione manuale di tali componenti per l'utilizzo di TLS non è consentita nella configurazione valutata.
- Il server e il client FTP di z/OS possono supportare sia i protocolli dello standard *draft* per la protezione dell'FTP con TLS, sia i protocolli del livello di sicurezza formale definito nel documento RFC 4217.
- FTP con TLS: questa valutazione ha preso in considerazione solo il livello di supporto formale del documento RFC 4217 e di conseguenza tale opzione deve essere utilizzata nella configurazione valutata.
- Se utilizzato, IPSec (IP Security) deve utilizzare le *suite* di cifratura elencate nell'SFR FCS_TLSC_PLUS.1.

RACF:

- Non utilizzare la RACF Remote Sharing Facility (RRSF) in modalità remota. Se si usa RRSF in modalità locale, assicurarsi che i comandi impartiti non possano essere utilizzati per eseguire una delle seguenti azioni:
    - assicurarsi che la classe RRFSFDATA non sia attiva;
    - definire il profilo DIRECT.* nella classe RRSFDATA con UACC(NONE) e nessun utente nella *access list*.
- Non utilizzare l'autenticazione a più fattori. Si può disabilitare l'autenticazione a più fattori rendendo la classe MFADEF inattiva.

Qualsiasi client fornito con il prodotto che viene eseguito con i privilegi dell'utente deve essere utilizzato con attenzione, poiché il TSF non può proteggere questi client da programmi potenzialmente ostili.

Le password/*passphrase* che un utente immette in questi programmi client e che questi client passano al server corrispondente per autenticare l'utente potrebbero essere potenzialmente falsificate da programmi ostili in esecuzione nello spazio degli indirizzi dell'utente. Ciò include, ad esempio, programmi client per Telnet, TN3270, FTP, *r-commands* e utilità di amministrazione `ssh` che richiedono all'utente di inserire la propria password/*passphrase*. Quando si utilizzano questi programmi client, l'utente deve fare attenzione che nessun programma potenzialmente ostile non attendibile sia stato chiamato nella sua stessa sessione.

I seguenti elementi e componenti di elementi non possono essere utilizzati in un sistema valutato, o perché violano le politiche di sicurezza indicate nel Traguardo di Sicurezza [TDS] o perché non sono stati inclusi nella configurazione valutata. Poiché fanno parte del sistema di base, o non devono essere configurati per l'uso oppure devono essere disattivati, come descritto nel capitolo 7 ("The evaluated configuration for the Common Criteria") del documento [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 per z/OS HTTP Server V7.0.

Inoltre, le seguenti funzionalità e servizi non possono essere utilizzati nella configurazione valutata:

- I componenti Advanced Program-to-Program Communication / Multiple Virtual Storage (APPC/MVS) del BCP.
- Il DFSMS Object Access Method per le applicazioni di tipo *content management*.

- Il servizio RACF remote sharing in modalità remota.
- Comunicazione JES2 NJE via TCP/IP. JES2 NJE deve utilizzare SNA o BSC nella configurazione valutata.
- Il servizio JES2 Execution Batch Monitor (XBM).
- La maggior parte delle funzioni dell'Enterprise Identity Mapping (EIM). Per maggiori dettagli, consultare il documento [MLSGUIDE].

9.3.2 Installazione e configurazione dell'hardware

L'ODV è un'istanza di z/OS in esecuzione su una macchina astratta come unico sistema operativo e che esercita il pieno controllo su questa macchina astratta. La macchina astratta, la maggior parte della quale non fa parte dell'ODV, può essere fornita da:

- una partizione logica fornita da una versione certificata di PR/SM in esecuzione su IBM z15 con CPACF DES/TDES Enablement Feature 3863 attivo, con schede Crypto Express7S;
- una versione certificata di IBM z/VM® in esecuzione in una partizione logica fornita da PR/SM su processori System z™.

Le seguenti periferiche possono essere utilizzate con l'ODV, pur preservandone le funzionalità di sicurezza:

- tutti i terminali supportati dall'ODV;
- tutte le stampanti supportate dall'ODV;
- tutti i dispositivi di memorizzazione e backup supportati dall'ODV;
- tutti gli adattatori di rete Ethernet e *token-ring* supportati dall'ODV.

Nota: le periferiche possono essere virtualizzate nel caso di ODV in esecuzione all'interno di una partizione logica o di z/VM. Il software di partizione logica e il software z/VM fa parte della macchina astratta e quindi dell'ambiente dell'ODV. La documentazione del software di partizionamento logico e la documentazione di z/VM forniscono la guida richiesta su come impostare e configurare il software di partizionamento logico o z/VM e come definire i dispositivi periferici logici in modo che l'ODV operi in modo sicuro nel partizionamento logico o nell'ambiente z/VM.

La configurazione hardware è ulteriormente dettagliata nel par. 1.5.3.2 del Traguardo di Sicurezza [TDS].

10 Appendice B – Configurazione valutata

L'ODV è il prodotto "z/OS Version 2 Release 4" sviluppato dalla società IBM Corporation. L'ODV è composto unicamente da software ed è accompagnato dalla documentazione di guida. Gli elementi elencati in Tabella 2 rappresentano l'ODV.

Il Pacchetto Base z/OS V2R4 Common Criteria nella configurazione valutata deve essere installato in base alle indicazioni nel par. 9.3.1 per le parti SW ed alle indicazioni nel par. 9.3.2 per le parti HW.

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 EAL4, con 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 richiede che i pacchetti software che compongono l'ODV siano eseguiti su una macchina astratta che implementa l'interfaccia della macchina z/Architecture come definito in "z/Architecture Principles of Operation" ([ZARCH]). Le piattaforme hardware che implementano questa macchina astratta sono le seguenti:

- IBM z15 con CPACF DES/TDES Enablement Feature 3863 attivo, con schede Crypto Express7S.

Si noti che le schede Crypto Express sopra menzionate non fanno parte dell'ODV e pertanto l'implementazione delle funzioni crittografiche fornite da tali schede non è stata valutata. Sono stati eseguiti test utilizzando tali schede per garantire che le funzioni crittografiche fornite da tali schede funzionino in linea di principio. Non è stata eseguita alcuna analisi di vulnerabilità o analisi *side channe*l per tali funzioni crittografiche. Le dichiarazioni fatte nel Traguardo di Sicurezza in merito alle funzioni crittografiche si applicano solamente alle funzioni implementate dal software.

L'ODV può essere eseguito su macchine all'interno di una partizione logica fornita da una versione certificata di IBM PR/SM. Inoltre, l'ODV può essere eseguito su una macchina virtuale fornita da una versione certificata di IBM z/VM.

Per le periferiche che possono essere utilizzate con l'ODV, fare riferimento al par. 1.5.3.2 del Traguardo di Sicurezza [TDS].

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

Sui sistemi di test è stato eseguito z/OS Version 2 Release 4 nella configurazione valutata. A causa dell'enorme quantità di test, questi sono stati eseguiti durante lo sviluppo dell'ODV. Per garantire un test adeguato di tutti i comportamenti rilevanti per la sicurezza dell'ODV, i Valutatori hanno verificato che tutti i test che avrebbero potuto essere interessati da qualsiasi modifica rilevante per la sicurezza introdotta successivamente nel ciclo di sviluppo erano stati eseguiti sulla configurazione valutata.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Approccio adottato per i test

IBM testa le piattaforme per z/OS individualmente rispetto alla conformità a z/Architecture utilizzando la suite di test Systems Assurance Kernel (SAK). Questi test assicurano che ogni piattaforma fornisca l'interfaccia della macchina astratta necessaria per l'esecuzione di z/OS. Il test SAK è importante non solo per la valutazione di z/OS, ma anche per altre valutazioni (PR/SM, z/VM).

I Functional Verification Tests (FVT) per z/OS vengono in gran parte eseguiti sul sistema di test VICOM. Questo è un sistema z/VM avanzato che implementa l'interfaccia di macchina astratta z/Architecture. Consente agli operatori di visualizzare singole macchine di prova virtuali 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. Il driver di test BERD (Background Environment Random Driver) invia i casi di test come job JES2. L'orientamento di IBM è di spostare sempre più test in questo ambiente automatizzato, il che faciliterà sostanzialmente l'impegno richiesto per i test per le successive valutazioni. A partire dalla V1R9 è stato portato un numero considerevole di test 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.

I sistemi di test hanno eseguito z/OS Version 2 Release 4 nella configurazione valutata. Il Fornitore ha messo a disposizione un'immagine di sistema preinstallata per VICOM e per le macchine che eseguono i test COMSEC, assicurando così che la versione del software CCEB fosse utilizzata per tutti i test. Le PTF aggiuntive sono state applicate ai sistemi VICOM e COMSEC non appena disponibili.

L'approccio generale per i test di IBM è definito nel processo di Integrated Product Development (IPD) con test per gli sviluppatori, test di verifica funzionale (FVT) e test di verifica del sistema (SVT). Per ogni versione, uno sforzo complessivo di oltre 100 anni persona viene dedicato a FVT e SVT per i componenti z/OS. FVT e SVT vengono eseguiti da team di test indipendenti, con operatori indipendenti dal Fornitore. I diversi team di test hanno sviluppato i propri strumenti di documentazione di test e test individuali, ma tutti implementano i requisiti stabiliti nella documentazione IPD.

Ai fini della valutazione, FVT è di interesse per i Valutatori, poiché qui vengono testate le singole funzioni di sicurezza dichiarate nel Traguardo di Sicurezza [TDS]. IBM ha deciso di creare un gruppo di test 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 affrontare la complessità altrimenti schiacciante dei test di z/OS.

La strategia di test di IBM per la valutazione è basata su tre capisaldi:

- La principale interfaccia di sicurezza interna è l'interfaccia per RACF, che è stata testata in modo esaustivo dal gruppo di test RACF.

- I componenti che richiedono servizi di identificazione e autenticazione o di controllo di accesso richiamano RACF. Per la maggior parte di questi servizi è stato sufficiente dimostrare che queste interfacce chiamano RACF, una volta che il test dell'interfaccia RACF (vedi sopra) ha verificato 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 dell'operatore, determinati servizi richiamabili, routine SVC e PC, i test hanno stabilito unicamente che queste interfacce non possono essere richiamate da chiamanti non autorizzati.

Oltre a questi test, tutti i componenti che forniscono interfacce esterne per le funzioni di sicurezza sono stati testati estensivamente. Per l'attuale versione di z/OS sono stati inclusi test aggiuntivi per via di aggiornamenti di componenti dell'ODV già esistenti. Tutti i nuovi casi di test 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

Il Fornitore ha messo a disposizione una mappatura tra le TSF del Traguardo di Sicurezza [TDS], le TSFI nelle specifiche funzionali e i test eseguiti. I Valutatori hanno verificato questa mappatura ed esaminato i casi di test per verificare se i test coprissero le funzioni e le loro interfacce. Sebbene non fossero richiesti test approfonditi, il Fornitore ha dato prova del fatto che sono stati testati dettagli significativi delle funzioni di sicurezza.

I Valutatori hanno stabilito che i test del Fornitore hanno garantito la copertura richiesta. I test hanno riguardato tutte le TSF identificate nel Traguardo di Sicurezza su tutte le interfacce identificate nelle specifiche funzionali.

La profondità del 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 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 al loro interno.

- Per le funzioni crittografiche, il supporto hardware fornito dall'ambiente IT dell'ODV è accessibile tramite il componente ICSF.

- 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 e sui sottosistemi che invocano RACF.

11.2.3 Risultati dei test

I risultati dei test del Fornitore sono stati generati sulle configurazioni come descritto in precedenza. Sebbene diversi team di test abbiano utilizzato strumenti e database di monitoraggio dei test diversi, i Valutatori hanno verificato che tutti i risultati forniti mostravano che i test erano stati eseguiti con successo e avevano prodotto i risultati attesi.

I Valutatori hanno verificato che l'attività di test è stata eseguita su configurazioni conformi al TDS, ad eccezione di un certo numero di patch, che sono state accettate dai Valutatori dopo averne esaminato il potenziale impatto.

I Valutatori sono stati in grado di seguire e comprendere appieno l'approccio dei test basandosi sulle informazioni messe a disposizione dal Fornitore.

Tramite questo ambiente di test, il Fornitore è stato in grado di dimostrare ai Valutatori la copertura e la profondità dei test necessarie. Di fatto, IBM ha fornito ai Valutatori solo una piccola parte dei test complessivi, in considerazione della complessità della valutazione. I Valutatori si sono convinti, in base alla loro esperienza nel lavorare a stretto contatto con gli operatori per un lungo periodo di tempo, che la copertura complessiva e la profondità dei test eseguiti da IBM sulle funzioni di sicurezza erano maggiori della parte mostrata ai Valutatori.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

11.3.1 Approccio adottato per i test

I test indipendenti dei Valutatori hanno seguito la guida CEM per verificare ogni funzione di sicurezza, senza ripetere in maniera esaustiva tutti i test del Fornitore.

Affinché la serie di test del Fornitore potesse essere rieseguita e osservata, i Valutatori hanno scelto un approccio che integrasse i loro test e si concentrasse sulle funzionalità modificate rispetto alla valutazione precedente.

I Valutatori hanno deciso di concentrarsi sulle funzioni di sicurezza dichiarate nel Traguardo di Sicurezza [TDS].

I Valutatori hanno acquisito fiducia nell'approccio del Fornitore per l'esecuzione dei test durante sessioni dedicate organizzate per consentire ai Valutatori di osservare gli operatori che eseguivano i test.

Tutti i test dei Valutatori sono stati eseguiti sul sistema di test VICOM che è stato configurato dai Valutatori secondo le specifiche indicate nella guida [MLSGUIDE]. Un'eccezione a questo approccio ha riguardato le patch aggiuntive, consigliate dal Fornitore per l'ODV, anche se non facevano parte della configurazione CC per i test. I Valutatori hanno tuttavia accettato tale deviazione fornendo una giustificazione adeguata nel rapporto di attività della classe ATE. Un altro elemento relativo alla configurazione, rilevato dai Valutatori, ha riguardato il fatto che le macchine di test COMSEC del Fornitore includevano componenti che non facevano parte dell'ambito della valutazione (componenti come ad esempio Kerberos erano installati su questi sistemi). Anche questo è stato ritenuto accettabile, in quanto ha solo aumentato l'interfaccia disponibile, senza influire sulle funzionalità di sicurezza dichiarate.

11.3.2 Copertura dei test

Per i propri test, i Valutatori hanno deciso di concentrarsi su diversi tipi di funzioni di sicurezza dell'ODV al fine di fornire una verifica indipendente del loro corretto funzionamento:

- Identificazione e autenticazione: i Valutatori hanno elaborato solo alcuni test di base delle funzioni di identificazione e autenticazione per TSO/E (password, *passphrase*) ed SSH e l'applicazione del *timeout* della console. È stato esteso un nuovo test per la verifica dell'usabilità di nomi utente più lunghi di 8 caratteri, restrizione applicata da lungo tempo. Inoltre, mentre sperimentavano la gestione degli utenti e i comandi TSO, i Valutatori hanno inizialmente riscontrato un comportamento apparentemente inaspettato delle funzioni di gestione degli utenti non RACF (account UADS), che hanno poi ulteriormente analizzato e testato.

- Sicurezza delle comunicazioni: i Valutatori hanno scelto di verificare che il canale di comunicazione sicuro SSH implementasse tutte gli algoritmi di cifratura dichiarati, gli HMAC e gli algoritmi di scambio di chiavi.

- Autorizzazione comando operatore RACF: verifica della protezione predefinita dei comandi operatore RACF contro l'utilizzo da parte di utenti non privilegiati.

- Gestione della sicurezza: i Valutatori hanno deciso di non ideare test speciali per questo caso, in quanto la configurazione dell'ambiente di test e l'impostazione/pulizia dei test avrebbe incluso già una parte consistente di questa TSF.

- Audit: i Valutatori hanno verificato che la modifica dell'orologio creava record di audit corrispondenti.

- Autoprotezione dell'ODV: l'unica funzione che è stato possibile testare in maniera adeguata è stata il riutilizzo degli oggetti, al cui riguardo i Valutatori hanno deciso di concentrarsi sul problema delle pagine di memoria probabilmente contenenti informazioni residue. Tutte le altre caratteristiche di autoprotezione sono proprietà che non possono essere facilmente messe alla prova dai test dei Valutatori.

11.3.3 Risultati dei test

Tutti i casi di test ideati dai Valutatori sono stati svolti con esito positivo. Tutti i test hanno fornito risultati corrispondenti a quelli previsti.

Non ci sono stati test falliti causati da comportamenti dell'ODV diversi da quelli previsti o in violazione dei requisiti indicati nel Traguardo di Sicurezza [TDS].

11.4 Analisi delle vulnerabilità e test di intrusione

11.4.1 Approccio adottato per i test

I Valutatori hanno analizzato il Traguardo di Sicurezza [TDS], la documentazione di progettazione ed i risultati dei test per individuare potenziali vulnerabilità. Inoltre, i Valutatori hanno effettuato una ricerca su fonti pubbliche per potenziali vulnerabilità note o dichiarate dell'ODV o di componenti dell'ODV. Tali ricerche non hanno rivelato alcun candidato evidente per i test di intrusione. Inoltre, le nuove funzionalità dichiarate nel Traguardo di Sicurezza erano troppo semplici da implementare per essere un buon candidato per test di intrusione.

I Valutatori, anche sulla base delle discussioni avute con il team interno di analisi di vulnerabilità di IBM, hanno ideato alcuni test di intrusione mirati a funzioni che non erano nuove per questa versione dell'ODV.

11.4.2 Copertura dei test

11.4.2.1 Attacco a chiamate di sistema legacy

Una prima serie di test di intrusione ha riguardato le chiamate di sistema *legacy* che ancora esistono in z/OS per mantenere la compatibilità anche con versioni molto vecchie dell'ODV. Alcune di queste chiamate di sistema non vengono più utilizzate dai programmi sviluppati di recente poiché le nuove funzioni forniscono un supporto migliore per gli sviluppatori di applicazioni. Le chiamate di sistema *legacy* potevano quindi non essere state modificate da molti anni e, a causa del loro utilizzo principalmente da parte di programmi *legacy*, le vulnerabilità all'interno di tali chiamate di sistema potevano non essere state rilevate e segnalate negli ultimi anni.

Un problema riscontrato in passato per alcune di queste chiamate di sistema *legacy* è il controllo incompleto dei diritti di accesso di un chiamante alle posizioni di memoria i cui indirizzi vengono passati alla chiamata di sistema. Se una posizione di memoria è protetta dall'accesso per i programmi utente, una funzione di chiamata di sistema (che non è soggetta alla protezione dall'accesso) può rivelare informazioni sul contenuto dell'archiviazione protetta dall'accesso se utilizza la memoria senza prima verificare se il chiamante è autorizzato a leggere i dati da quella posizione di memoria.

Di norma una chiamata di sistema dovrebbe, prima di accedere alla memoria per conto del chiamante, controllare se il chiamante è autorizzato ad accedere a quella posizione di memoria. In caso contrario, la chiamata di sistema dovrebbe restituire un codice ABEND di violazione di accesso alla memoria.

Pertanto, è stato sviluppato un programma che ha permesso di controllare un certo numero di chiamate di sistema *legacy* passando l'indirizzo di memoria di un'area di archiviazione precedentemente identificata come protetta dall'accesso per il programma chiamante.

Il test di intrusione è stato eseguito su otto diverse chiamate di sistema *legacy*. Tutte hanno restituito il codice ABEND corretto per la violazione di accesso alla memoria.

11.4.2.2 Tentativo di esaurimento della memoria

È stato sviluppato ed eseguito un secondo test di intrusione che ha tentato di esaurire la memoria utilizzata internamente dall'ODV facendo in modo che un programma creasse il maggior numero possibile di blocchi di controllo di sistema specifici (in questo caso Task Control Blocks) creando nuovi task in un ciclo infinito. Questo test di intrusione ha dimostrato che l'ODV è protetto da tale attacco e limita il numero di task che possono essere creati all'interno di uno spazio di indirizzi.

11.4.2.3 Attacco al cambio di password

È stato creato un terzo test di intrusione per verificare una potenziale *race condition* quando un utente è costretto dall'amministratore a modificare la propria password. Partendo dal presupposto che la password temporanea assegnata dall'amministratore potesse essere nota a un utente malintenzionato, è stato sviluppato ed eseguito un test di intrusione in cui due persone (un intruso oltre all'utente legittimo) hanno effettuato l'accesso all'ODV utilizzando la password temporanea. Se avesse funzionato, a entrambi gli utenti sarebbe stato chiesto di cambiare la password. Il test ha dimostrato che l'ODV vieta il secondo login consentendo così ad un solo utente alla volta di autenticarsi con lo stesso ID, vanificando così l'attacco.

11.4.3 Risultati dei test

In tutti i casi i test di intrusione si sono conclusi con un messaggio di errore che mostrava il corretto funzionamento dell'ODV.

Nel caso delle chiamate di sistema SVC *legacy* testate per controllare correttamente il diritto di accesso del chiamante alle posizioni di memoria passate come parametro, tutte le SVC testate sono terminate con un codice ABEND di 0C4 che indica che è stata rilevata una violazione di accesso alla memoria.

Nel caso del programma "Rabbit" di creazione di task (e relativi blocchi di controllo dei task nello spazio di sistema), l'ODV ha terminato il programma con un messaggio di errore in cui affermava di aver rilevato un esaurimento nello spazio di sistema.

Nel caso del test di modifica della password, al secondo accesso che utilizzava un percorso di accesso diverso è stato impedito di modificare la password rivelando che l'ODV ha correttamente riconosciuto che era già in corso una modifica della password.

11.4.4 Vulnerabilità residue

I Valutatori hanno eseguito la loro analisi di vulnerabilità anche sulla base delle informazioni fornite nel Traguardo di Sicurezza [TDS], nella documentazione di progetto, nella rappresentazione dell'implementazione e nella guida per l'utente. I Valutatori non

hanno riscontrato alcuna nuova vulnerabilità introdotta da funzionalità nuove o modificate in z/OS V2R4 che possa essere sfruttata nell'ambiente operativo dell'ODV. Nessuna vulnerabilità è stata riscontrata nelle fonti pubbliche verificate dai Valutatori (CVE, la mailing list RACF specifica per z/OS, ricerche generali su Internet).

Vale la pena evidenziare che nella valutazione della precedente versione dell'ODV z/OS V2R3 ([RC]) erano state rilevate due vulnerabilità residue (CVE-2018-0734, CVE-2018-0735). Con la nuova implementazione scelta da IBM per le funzioni crittografiche interessate, queste vulnerabilità sono state rimosse dalla versione corrente dell'ODV.