Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

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. 6/19

(Certification No.)

Prodotto: **IBM 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:

EAL4+
(ALC_FLR.3)

Il Direttore
(Dott.ssa Eva Spina)

Roma, 31 luglio 2019

Common Criteria

Fino a EAL2 *(Up to EAL2)*

Questa pagina è lasciata intenzionalmente vuota

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

IBM z/OS Version 2 Release 3

OCSI/CERT/ATS/01/2018/RC

Versione 1.0

31 luglio 2019

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	31/07/2019

2 Indice

1 Revisioni del documento 5
2 Indice 6
3 Elenco degli acronimi 8
4 Riferimenti 10
5 Riconoscimento del certificato 12
5.1 Riconoscimento di certificati CC in ambito internazionale (CCRA) 12
6 Dichiarazione di certificazione 13
7 Riepilogo della valutazione 14
7.1 Introduzione 14
7.2 Identificazione sintetica della certificazione 14
7.3 Prodotto valutato 14
7.3.1 Architettura dell'ODV 15
7.3.2 Caratteristiche di Sicurezza dell'ODV 18
7.3.3 Funzioni crittografiche 22
7.4 Documentazione 24
7.5 Conformità a Profili di Protezione 24
7.6 Requisiti funzionali e di garanzia 24
7.7 Conduzione della valutazione 25
7.8 Considerazioni generali sulla validità della certificazione 25
8 Esito della valutazione 27
8.1 Risultato della valutazione 27
8.2 Raccomandazioni 28
9 Appendice A – Indicazioni per l'uso sicuro del prodotto 29
9.1 Consegna dell'ODV 29
9.2 Identificazione dell'ODV 31
9.3 Installazione, inizializzazione ed utilizzo sicuro dell'ODV 31
9.3.1 Installazione e configurazione del SW 31
9.3.2 Installazione e configurazione dell'HW 36
10 Appendice B – Configurazione valutata 37
11 Appendice C – Attività di Test 38

11.1 Configurazione per i Test 38
11.2 Test funzionali svolti dal Fornitore 39
11.2.1 Approccio adottato per i test 39
11.2.2 Copertura dei test 40
11.2.3 Risultati dei test 41
11.3 Test funzionali ed indipendenti svolti dai Valutatori 41
11.3.1 Approccio adottato per i test 41
11.3.2 Copertura dei test 42
11.3.3 Risultati dei test 43
11.4 Analisi delle vulnerabilità e test di intrusione 43
11.4.1 Approccio adottato per i test 43
11.4.2 Copertura dei test 43
11.4.3 Risultati dei test 44
11.4.4 Vulnerabilità residue 44

3 Elenco degli acronimi

AES	Advanced Encryption Standard
APAR	Authorized Program Analysis Report
API	Application Programming Interface
BCP	Base Control Program
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CPACF	Central Processor Assist for Cryptographic Function
cPP	collaborative Protection Profile
DAC	Discretionary Access Control
DASD	Direct Access Storage Device
DES	Data Encryption Standard
DFSMS	Data Facility Storage Management Subsystem
DPCM	Decreto del Presidente del Consiglio dei Ministri
DVD	Digital Versatile Disk
EAL	Evaluation Assurance Level
ICSF	Integrated Cryptographic Service Facility
ID	Identifier
IPL	Initial Program Load
IUCV	Inter User Communication Vehicle
IT	Information Technology
JES2	Job Entry System 2
LDAP	Lightweight Directory Access Protocol
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
PKI	Public Key Infrastructure
PP	Protection Profile
PR/SM	Processor Resource/System Manager
PTF	Program Temporary Fix
RACF	Resource Access Control Facility
SAK	System Assurance Kernel
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SMF	System Management Facilities
SHA	Secure Hash Algorithm
SRB	Service Request Block
SSL	Secure Sockets Layer
SSH	Secure SHell
TCP/IP	Transmission Control Protocol/Internet Protocol
TDS	Traguardo di Sicurezza
TLS	Transport Layer Security
TSF	TOE Security Functionality
TSFI	TSF Interface
TSO	Time Sharing Option
USS	UNIX System Services

4 Riferimenti

[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

[ETR] Final Evaluation Technical Report “IBM z/OS Version 2 Release 3”, OCSI-CERT-ATS-01-2018_ETR_190614_v3, Version 3, atsec information security GmbH, 14 June 2019

[ETR-TEST] Evaluation Technical Report - Assurance Class ATE, Version: 3, Date: 2019-04-18

[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

[OSPP] Operating System Protection Profile, Version 2.0, BSI-CC-PP-0067, 01 June 2010

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

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

[MLSGUIDE] z/OS Version 2 Release 3 - Planning for Multilevel Security and the Common Criteria, Version: GA32-0891-30, Date: 2019-05-15

[RFC4217] “Securing FTP with TLS”, October 2005

[TDS] IBM z/OS Version 2 Release 3 Security Target, Version 12.10, IBM Corporation, 25 February 2019

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

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 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 z/OS Version 2 Release 3", sviluppato dalla società International Business Machines Corp. (IBM).

z/OS Version 2 Release 3 (indicato nel seguito anche come z/OS V2R3 o z/OS) è un sistema operativo multiutente, general-purpose, multi-tasking 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).

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 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.

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 operativo previsto.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	IBM z/OS Version 2 Release 3
Traguardo di Sicurezza	IBM z/OS Version 2 Release 3 Security Target, Version 12.10 [ST]
Livello di garanzia	EAL4 con l'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	Operating System Protection Profile v2.0 [OSPP] con gli Extende Package (EP) [OSPP-LS] e [OSPP-EIA].
Data di inizio della valutazione	13 Febbraio 2019
Data di fine della valutazione	17 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 paragrafo vengono sintetizzate le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'Oggetto della Valutazione (ODV) è z/OS Version 2 Release 3 con i seguenti elementi:

- z/OS Version 2 Release 3 (V2R3).

- IBM Print Services Facility™ Version 4 Release 5 for z/OS.
- Overlay Generation Language Version 1 Release 1.

z/OS è un sistema operativo multiutente, general-purpose, multi-tasking per sistemi di elaborazione aziendali. Più utenti possono utilizzare z/OS simultaneamente per eseguire una varietà di funzioni che richiedono un accesso controllato e condiviso alle informazioni memorizzate nel sistema.

z/OS può essere configurato per due modalità operative, una modalità Standard Mode ed una modalità Labeled Security Mode.

Il Traguardo di Sicurezza [TDS] su cui si è basata l'attività di valutazione è conforme al Profilo di Protezione certificato "Operating System Protection Profile (OSPP)" [OSPP] ed ai suoi pacchetti estesi Labeled Security ([OSPP-LS]) e Extended Identification and Authentication ([OSPP-EIA]).

I requisiti di sicurezza dell'ODV si basano interamente sui componenti di garanzia definiti nella parte 3 dei criteri comuni ([CC]). z/OS soddisfa i requisiti di garanzia per il livello di garanzia di valutazione EAL4 con l'aggiunta di ALC_FLR.3.

I Requisiti funzionali di sicurezza (SFR) relativi all'ODV sono descritti nel Traguardo di Sicurezza [TDS], sezione 7.1. Questi sono selezionati da Common Criteria Part 2 e da OSPP, dove alcuni SFR sono stati definiti come componenti estesi. Pertanto, z/OS è esteso rispetto a CC parte 2. Ci sono anche requisiti relativi all'ambiente operativo dell'OSD che sono rappresentanti seguendo notazione SFR-tipo nel traguardo di sicurezza ([TDS], capitolo 6)

Le funzioni di sicurezza dell'ODV sono descritte con maggiore dettaglio nel capitolo 7.3.2.3.

Per ulteriori dettagli sulla versione del software, la definizione del ODV, la macchina astratta su cui è eseguito l'ODV e la documentazione di guida per l'utente consegnata con l'ODV, fare riferimento al resto di questo rapporto.

7.3.1 Architettura dell'ODV

7.3.1.1 Panoramica generale dell'ODV

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. Questa macchina astratta, la maggior parte della quale non fa parte dell'ODV, può essere fornita attraverso una delle opzioni nella sezione 0.

Istanze multiple di z/OS possono essere collegate in due modi, ovvero in un *sysplex* di base o in un *sysplex* parallelo con le istanze che condividono il loro database RACF (Resource Access Control Facility). Le singole istanze di z/OS possono essere eseguite da sole o all'interno di una rete come un insieme di host cooperanti, che operano e implementano lo stesso insieme di politiche di sicurezza. Per ulteriori dettagli, consultare il Traguardo di Sicurezza [TDS].

La macchina astratta definita dalla z/Architecture non fa parte dell'ODV, appartiene invece all'ambiente operativo dell'ODV. Tuttavia, la correttezza dei meccanismi di separazione e protezione della memoria implementati nella macchina astratta sono analizzati come parte della valutazione, poiché tali funzioni sono cruciali per la sicurezza dell'ODV. Le istruzioni crittografiche che implementano gli algoritmi AES, Triple-DES, SHA-1 e SHA-2 fornite dalla funzione CPACF del processore sono state analizzate nella valutazione per verificare il corretto supporto alle TSF.

I servizi di rete, i collegamenti e le comunicazioni di TCP/IP (Transmission Control Protocol/Internet Protocol) che si verificano al di fuori di un *sysplex* sono limitati a un'etichetta di sicurezza; vale a dire, ogni sistema considera i suoi pari come host con etichetta singola. Altre comunicazioni di rete non sono consentite, ad eccezione del protocollo JES2 (Job Entry System 2) NJE (Network Job Entry).

La maggior parte delle funzioni di sicurezza dell'ODV (TSF) sono fornite dal Base Control Program (BCP) del sistema operativo z/OS e da RACF, componente z/OS utilizzato da diversi servizi come istanza centrale per l'identificazione e autenticazione e per le decisioni di controllo degli accessi. z/OS viene fornito con funzioni di gestione che consentono la configurazione delle funzioni di sicurezza dell'ODV per adattarle alle esigenze del cliente.

Alcuni elementi che non forniscono funzioni di sicurezza sono stati inclusi nell'ODV. Questi elementi funzionano in modalità autorizzata, quindi potrebbero compromettere l'ODV se non si comportano correttamente. Poiché questi elementi sono essenziali per il funzionamento di molti ambienti dei clienti, l'inclusione di questi elementi li sottopone al processo di controllo durante la valutazione per garantire che possano essere utilizzati dai clienti senza influire sullo stato di sicurezza dell'ODV.

Nella sua configurazione valutata, z/OS Version 2 Release 3 consente due modalità operative: una modalità standard che soddisfa tutti i requisiti di base del profilo di protezione del sistema operativo [OSPP] e il suo pacchetto esteso Extended Identification and Authentication [OSPP-EIA] e una modalità più restrittiva denominata Labeled Security Mode, che soddisfa inoltre tutti i requisiti del pacchetto esteso OSPP Labeled Security [OSPP-LS]. In entrambe le modalità, vengono utilizzati gli stessi elementi software. Le due modalità hanno impostazioni di RACF diverse rispetto all'uso delle etichette di sicurezza. Tutti gli altri parametri di configurazione sono identici nelle due modalità.

La funzionalità CPACF è fornita dalle istruzioni del processore della macchina astratta sottostante, che sono trattate come parte delle TSF. La funzionalità crittografica fornita dai coprocessori crittografici specifici su schede CryptoExpress non fa parte dell'ODV.

Le funzioni crittografiche implementate dai coprocessori CEX3, CEX4, CEX5 o CEX6 fanno anch'esse parte dell'ambiente operativo dell'ODV e pertanto non sono state valutate nella misura richiesta dal livello di garanzia previsto in questa valutazione. Per utilizzare solo le funzioni crittografiche fornite dall'ODV, l'utente deve configurare l'ODV in modo tale che non sia installato alcun coprocessore crittografico o che l'uso di tali funzioni sia disabilitato.

Un utente che desidera utilizzare le funzioni crittografiche fornite da un coprocessore dovrebbe essere consapevole del fatto che, sebbene tali funzioni siano state testate durante la valutazione rispetto alla correttezza funzionale, non sono state eseguite ulteriori analisi della progettazione e dell'implementazione di tali funzioni crittografiche

implementate sui coprocessori in questa valutazione. In particolare, non è stata eseguita alcuna analisi sui side-channel potenzialmente sfruttabili nell'implementazione delle funzioni crittografiche dei coprocessori.

7.3.1.2 Principali componenti software dell'ODV

z/OS Version 2 Release 3 include i seguenti sottosistemi principali:

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

- **System Management Facilities (SMF)**: SMF raccoglie e registra le informazioni relative al sistema ed 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 degli accessi 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'SMF audit).

- **Integrated Cryptographic Service Facility (ICSF)**: ICSF è il principale fornitore di servizi crittografici di base all'interno 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 dell'utente ed anche i certificati utilizzati nella creazione di canali fidati.

- **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, Communications Server offre: controllo degli accessi sugli oggetti, canali fidati, funzionalità di filtro IP.

- **Directory Services**: il server LDAP (Lightweight Directory Access Protocol), parte di IBM Tivoli Directory Server per z/OS (IBM), si basa su un modello client/server che fornisce l'accesso client a un server LDAP. Una directory LDAP fornisce un modo semplice per conservare le informazioni della directory in una posizione centrale per l'archiviazione, l'aggiornamento, il recupero e lo scambio.

- **Public Key Infrastructure (PKI)**: i servizi crittografici di z/OS consentono a z/OS di stabilire un'infrastruttura PKI e fungere da autorità di certificazione per utenti interni ed esterni, emettendo e amministrando certificati digitali in conformità con le politiche dell'organizzazione.

- **Job Entry System 2 (JES2)**: z/OS utilizza un sottosistema di inserimento di job (JES) per riceverli nel sistema operativo, programmarli per l'elaborazione da parte di z/OS e controllarne l'elaborazione degli output. JES2 discende da HASP (Houston automatic spooling priority). HASP è definito come un programma per computer che fornisce funzioni supplementari di gestione dei job, gestione dei dati e gestione delle attività come la pianificazione, il controllo del flusso di lavoro e lo spooling.

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

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

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

7.3.2 Caratteristiche di Sicurezza dell'ODV

7.3.2.1 Politica di sicurezza

I requisiti funzionali di sicurezza dell'ODV sono implementati dalle seguenti funzioni di sicurezza dell'ODV:

- Identificazione ed autenticazione,
- Controllo di accesso,
- Sicurezza della comunicazione,
- Gestione della sicurezza,
- Auditing,
- Riutilizzo degli oggetti,
- Protezione delle TSF,
- Protezione della riservatezza dei set di dati.

7.3.2.2 Obiettivi di sicurezza dell'ambiente operativo

I presupposti per il corretto funzionamento dell'ODV definiti nel Traguardo di Sicurezza [ST] ed alcuni aspetti riguardanti le minacce e le politiche di sicurezza organizzativa non sono coperti dall'ODV. Questi aspetti portano a specifici obiettivi di sicurezza che devono essere raggiunti dall'ambiente operativo dell'ODV. I seguenti obiettivi per l'ambiente operativo vanno in particolare assicurati:

- I responsabili dell'ODV sono competenti e affidabili.
- 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 il sistema sia distribuito, installato e configurato in modo sicuro.
- Gli utenti autorizzati dell'ODV devono garantire che i servizi diagnostici completi vengano invocati ad ogni periodo di manutenzione preventiva programmata.
- I responsabili dell'ODV devono garantire che le parti dell'ODV fondamentali per l'applicazione della politica di sicurezza siano protette dagli attacchi fisici.
- I responsabili dell'ODV devono garantire che siano fornite procedure e/o meccanismi per assicurare il ripristino del sistema da guasti o altre discontinuità.
- I sistemi IT attendibili remoti implementano i protocolli e i meccanismi richiesti dalle TSF per supportare l'applicazione della politica di sicurezza.

Per una descrizione completa degli obiettivi di sicurezza per l'ambiente operativo dell'ODV, fare riferimento alla sezione 4.2 del Traguardo di Sicurezza z/OS V2R3 [TDS].

7.3.2.3 Funzioni di sicurezza

I Requisiti Funzionali di Sicurezza dell'ODV sono realizzati dalle Funzioni di Sicurezza dell'ODV, sintetizzate nella Tabella 1. Per maggiori dettagli sulle funzionalità di sicurezza fornite dall'ODV si faccia riferimento al Traguardo di Sicurezza [TDS].

TOE Security Function	**implementation**
Identification and authentication	Alphanumeric RACF user ID and system-encrypted password or password phrase.
	Alphanumeric RACF user ID and PassTicket encompassing the user ID, the requested application name, and the current date/time.
	X.509v3 digital certificate with TLS-based client authentication mapped to a RACF user ID.
	Kerberos™ v5 ticket mapped through the TOE-provided GSS-API programming services or alternate functions mapped to a RACF user ID.
	LDAP LDBM bind DN or LDAP ICTX or SDBM bind DN together with a RACF password or password phrase mapped to RACF user ID and the password/phrase.
	Digital certificates presented to LDAP over TLS mapped to a RACF user ID.
Access Control	Discretionary Access Control (DAC): z/OS supports access controls that are capable of

TOE Security Function	implementation
	enforcing access limitations on individual users and data objects. Discretionary access control (DAC) allows individual users to specify how such resources as direct access storage devices (DASDs), tape data sets and tape volumes are to be shared.
	Mandatory Access Control (MAC): mandatory access control (MAC) functions are required for Labeled Security Mode, which impose additional access restrictions on information flow on security classification. Users and resources can have a security label specified in their profile. The access control ensures that users can only read labeled information if their security labels dominate the information's label, and that they can only write to labeled information containers if the container's label dominates the subject's, thus implementing the Bell-LaPadula model of information flow control. Security label checking will also occur in standard operation mode, if the administrator has configured security labels and if resources and users have labels assigned to them.
Communication security	z/OS provides means of secure communication between systems sharing the same security policy. z/OS TCP/IP provides the means for associating labels with all IP addresses in the network and for defining Virtual IP addresses (VIPAs) with specific labels on a multilevel system. z/OS TCP/IP considers the user's label when choosing a source address for communications. z/OS UNIX System Services also provides the means to run up to eight instances of the z/OS TCP/IP stack which can each be restricted to a single label. Either of these approaches can be used to ensure that most communications between multilevel systems do not use a multilevel address on both ends and thereby avoid the need for explicit labeling. TCP/IP-based communication can be further controlled by the access control function for TCP/IP connections, which allows controlling of the connection establishment based on access to the TCP/IP stack in general, individual network address and individual ports on a per-application or per-user basis. Additional means implemented in z/OS for securing the communication are • TLS v1.1 and v1.2 optionally with x.509-based client authentication • IPSec with IKE key exchange method • Kerberos™ version 5 networking protocols • OpenSSH, an SSH v2 implementation including ssh, scp and sftp
Security management	z/OS provides a set of commands and options to adequately manage its security functions, the capability of managing users, groups of users, general resource profiles, and RACF SETROPTS options via the z/OS LDAP server. z/OS also provides a Java class that allows Java programs to issue commands to manage users and groups. Both the LDAP and the Java class ultimately create a RACF command and pass it to RACF using a programming interface, and then RACF runs the command using the identity associated with the LDAP session or the Java program. z/OS recognizes several authorities that are able to perform the different management tasks related to the its security. Security administrators are in charge of managing general security options, MAC attributes, management, users and their security attributes and can delegate group security administrators or users to manage groups. Security administrators can define what audit records are captured by the system and auditors manage the parameters of the audit system and can analyze the audit trail. Users can change their own passwords or password phrases, their default groups, and their user names (but not their user IDs) and choose their security labels at login, for some login methods. Discretionary access rights to protected resources are managed by the owners of the applicable profiles (or UNIX objects) or by security administrators.
Auditing	The RACF component of z/OS provides a number of logging and reporting functions that allow resource owners and auditors to identify users who attempt to access resources. Audit records are collected by the System Management Facilities (SMF) into an audit trail, which is protected from unauthorized modification or deletion by the DAC and (in Labeled Security Mode) MAC mechanisms. In addition to writing records to the audit trail,

TOE Security Function	implementation
	messages can be sent to the security console to immediately alert operators of detected policy violations. RACF provides SMF records for all RACF-protected resources (either “traditional” or z/OS UNIX-based) as well as for LDAP-based resources. Remote applications can use an LDAP interface to request that RACF generate an SMF audit record. For reporting, auditors can unload all or selected parts of the SMF data for further analysis in a human-readable formats and can then upload the data to a query or reporting package, such as DFSORT™ if desired. The system can be configured to halt on exhaustion of audit trail space to prevent audit data loss. Operators are warned when audit trail space consumption reaches a predefined threshold.
Object reuse	Reuse of protected objects and of storage is handled by various hardware and software controls, and by administrative practices. All memory content of non-shared page frames is cleared before making it accessible to other address spaces or data spaces. DASD data sets can be purged during deletion with the RACF ERASE option and tape volumes can be erased on return to the scratch pool. All resources allocated to UNIX objects are cleared before reuse. Other data pools are under strict TOE control and cannot be accessed directly by normal users.
TSF protection	TSF protection is based on several protection mechanisms that are supported by the underlying abstract machine z/OS is executed upon. In addition to the protection mechanism of the underlying abstract machine, z/OS also uses software mechanisms like the authorized program facility (APF), specific privileges for programs in the UNIX system services environment to protect the TSF.
Confidentiality Protection of Data Sets	With z/OS confidentiality protection of data sets, users can encrypt data at rest without requiring application changes. z/OS data set encryption through RACF commands and SMS policies allows the administrator to identify the data sets or groups of data sets that require encryption. The administrator can specify an encryption key label, which refers to an encryption key. Both the key label and encryption key must exist in the ICSF key repository (CKDS). With data set encryption, the administrator is able to protect viewing the data in the clear. This is based on access to the key label that is associated with the data set and used by the access methods to encrypt and decrypt the data.

Tabella 1 – Funzioni di sicurezza dell’ODV

7.3.3 Funzioni crittografiche

Le Funzioni crittografiche sono elencate nella Tabella 2:

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level Above 100 Bits	Comments
CPACF						
1	Cryptographic Primitive (CPACF)	TDES in CFB, OFB, and CBC-CS modes	FIPS 46-3 (TDES), NIST Special Publication 800-38A, 2001 Edition (CFB and OFB modes of operation), Addendum to NIST SP 800-38A, October 2010 (CBC-CS mode of operation), NIST Special Publication 800-38D (GCM mode of operation) Note: the CBC-CS mode is implemented in accordance with [NIST-CBC-CS_PROP]. This mode is not used by the TSF for any security function claimed in the ST.	|k|=168	No	CPACF instructions
2	Cryptographic Primitive CPACF)	AES in CFB, OFB, and CBC-CS modes	FIPS 197 (AES), NIST Special Publication 800-38A, 2001 Edition (CFB and OFB modes of operation), Addendum to NIST SP 800-38A, October 2010 (CBC-CS mode of operation), NIST Special Publication 800-38D (GCM mode of operation)	|k|=128, 192, 256	yes	CPACF instructions
3	Cryptographic Primitive (CPACF)	SHA-1	FIPS 180-4	none	No	CPACF instructions
4	Cryptographic Primitive (CPACF)	SHA-{224, 256, 384, 512}	FIPS 180-4	none	yes	CPACF instructions
ICSF/CLIC						
5	Cryptographic Primitive	RSA signature generation	[PKCS#1 v2.1] (RSA)	Moduluslength= 2048, 4096	yes	ICSF CSFPPKS/ CSFPPKS6 function (hashing not done by the function)
6	Cryptographic Primitive	RSA signature generation	[PKCS#1 v2.1] (RSA)	Moduluslength= 1024	No	ICSF CSFPPKS/ CSFPPKS6 function (hashing not done by the function)
7	Cryptographic Primitive	RSA key generation		Moduluslength= 2048, 4096	yes	ICSF CSFPGKP/CSFPGKP6 function
8	Cryptographic Primitive	RSA key generation		Moduluslength= 1024	No	ICSF CSFPGKP/CSFPGKP6 function
9	Cryptographic Primitive, Authentication	RSA signature verification, used by RACF for certificate based user authentication (which calls ICSF)	[PKCS#1 v2.1] (RSA)	Moduluslength= 2048, 4096	yes	ICSF CSFPPKV/ CSFPPKV6 function (hashing not done by the function) (primitive also used for certificate based user authentication)

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level Above 100 Bits	Comments
10	Cryptographic Primitive, Authentication	RSA signature verification, used by RACF for certificate based user authentication (which calls ICSF)	[PKCS#1 v2.1] (RSA)	Moduluslength= 1024	No	ICSF CSFPPKV/ CSFPPKV6 function (hashing not done by the function) (primitive also used for certificate based user authentication)
11	Cryptographic Primitive	DSA signature generation	[FIPS 180-4] (DSA)	Plength= 1024, Qlength= 160	No	ICSF CSFPPKS/ CSFPPKS6 function (hashing not done by the function)
12	Cryptographic Primitive	DSA signature verification	[FIPS 180-4] (DSA)	Plength= 1024, Qlength= 160	No	ICSF CSFPPKV/ CSFPPKV6 function (hashing not done by the function)
13	Cryptographic Primitive	ECDSA signature generation	[FIPS 180-4] (ECDSA)	Key sizes corresponding to the used NIST elliptic curves secp{224, 256, 384, 521}r1 (SEC2)	yes	ICSF CSFPPKS/ CSFPPKS6 function (hashing not done by the function)
14	Cryptographic Primitive	ECDSA signature verification	[FIPS 180-4] (ECDSA)	Key sizes corresponding to the used NIST elliptic curves secp{224, 256, 384, 521}r1 (SEC2)	yes	ICSF CSFPPKV/ CSFPPKV6 function (hashing not done by the function)
15	Cryptographic Primitive	ECDSA signature generation	[ISO 14888-3] (ECDSA) (RFC 5639) BrainPool curves	Key sizes corresponding to the used elliptic curves brainpoolP{224, 256, 320, 384, 512}r1	yes	ICSF CSFPPKS/ CSFPPKS6 function (hashing not done by the function)
16	Cryptographic Primitive	ECDSA signature verification	[ISO 14888-3] (ECDSA) (RFC 5639) BrainPool curves	Key sizes corresponding to the used elliptic curves brainpoolP{224, 256, 320, 384, 512}r1	yes	ICSF CSFPPKV/ CSFPPKV6 function (hashing not done by the function)
17	Key agreement	ECDH	[ISO 11770-3]	Key sizes corresponding to the used elliptic curves secp{224, 256, 384, 521}r1 (SEC2) and brainpoolP{224, 256, 320, 384, 512}r1 (RFC 5639)	yes	ICSF PKCS#11 CSFPDVK/CSFPDVK6 function
System SSL						
18	Cryptographic Primitive	DSA signature generation	[FIPS 180-4] (DSA, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)	L=1024, N=160	No	System SSL function gsk_sign_data
19	Cryptographic Primitive	DSA signature verification	[FIPS 180-4] (DSA, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)	L=1024, N=160	No	System SSL function gsk_verify_data
20	Trusted Channel	TLS V1.1	[RFC4346] (V1.1)	Various (depends on the cipher suite selected)	Depends on the cipher suite selected	
21	Trusted Channel	TLS V1.2	[RFC5246] (V1.2)	Various (depends on the cipher suite selected)	Depends on the cipher suite selected	
Communications Server 390 (CS390)						
22	Trusted Channel	IPSec	[RFC4301] through [RFC4305], [RFC4308], and [RFC4835]	Various (depends on the cipher suite selected)	Depends on the cipher suite selected	
OpenSSH						

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level Above 100 Bits	Comments
23	Authentication	RSA (SSH)	[RFC4253] (SSH)	Moduluslength= 2048, 4096	Yes	Implemented in the OpenSSL library
24	Authentication	DSA (SSH)	[RFC4253] (SSH)	L=1024, N=160	No	Implemented in the OpenSSL library
25	Key agreement	DH (SSH)	[RFC4253] (SSH)	Plength 1024	No	Implemented in the OpenSSL library
26	Key agreement	ECDH	[ISO 11770-3]	Key sizes corresponding to the used elliptic curves secp{224, 256, 384, 521}r1 (SEC2) and brainpoolP{224, 256, 320, 384, 512}r1 (RFC 5639)	yes	ICSF PKCS#11 CSFPDVK/CSF PDVK6 function
27	Key agreement	DH (SSH)	[RFC4253] (SSH)	Plength 1024	No	Implemented in the OpenSSL library
28	Trusted Channel	SSH V2	[RFC4250] (lists the RFCs defining SSH V2)	Various (depends on the cipher suite selected)	Depends on the cipher suite selected	

Tabella 2 – Funzioni crittografiche

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 seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel capitolo 8.2 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] dichiara conformità "strict" al Profilo di Protezione [OSPP] ed agli Extended Package [OSPP-LS] e [OSPP-EIA].

7.6 Requisiti funzionali e di garanzia

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.

Tutti i requisiti di garanzia (SAR) sono stati selezionati dai CC Part 3 [CC3] ed includono tutti i requisiti del pacchetto EAL4 con l'aggiunta di ALC_FLR.3.

Tutti i requisiti funzionali di sicurezza (SFR) sono stati selezionati o derivati per estensione dai CC Parte 2 [CC2]. In particolare, il traguardo di sicurezza dichiara conformità "strict" al

PP [OSPP] ed ai pacchetti estesi [OSPP-LS] e [OSPP-EIA]. Per quanto riguarda [OSPP], sono inclusi tre componenti estesi:

- FCS_RNG.1: Random number generation,
- FDP_RIP.3: Full residual information protection of subjects, and
- FIA_USB.2: Enhanced user-subject binding.

Per quanto riguarda [OSPP-EIA], sono inclusi due componenti estesi:

- FIA_UAU.8: Authentication policy decisions, e
- FIA_UID.3: Identification policy decisions.

Gli utenti devono fare riferimento Traguardo di sicurezza [TDS] per una descrizione completa di tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono affrontare, i requisiti funzionali di sicurezza (SFR) e le funzioni di sicurezza che realizzano gli stessi obiettivi.

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 17 giugno 2019 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [ETR] che è stato approvato dall'Organismo di Certificazione il 19 giugno 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 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 3" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, 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 3 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 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 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
Identification of security measures	ALC_DVS.1	Positivo

Classi e componenti di garanzia		Verdetto
Developer defined life-cycle model	ALC_LCD.1	Positivo
Well-defined development tools	ALC_TAT.1	Positivo
Systematic flaw remediation	*ALC_FLR.3*	Positivo
Test	**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 3 – 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 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]).

Si assume che l'ODV funzioni in modo sicuro qualora vengano rispettate le ipotesi sull'ambiente operativo descritte nel par. 4.2 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 si effettua un ordine tramite servizi Internet (protetti), IBM richiede ai clienti di avere un account con nome utente e password. La registrazione per tale account a sua volta richiede un ID cliente valido da IBM.

No	Type	Identifier	Release	Form of Delivery
z/OS Version 2 Release 3 (z/OS V2.3, program number1 5650-ZOS)[1] Common Criteria Evaluated Base Package				
1	SW	z/OS V2.3 Common Criteria Evaluated Base (IBM program number 5650-ZOS)	V2R3	Tape
2	DOC	z/OS V2.3 Program Directory	GI11-9848-02	Hardcopy
3	DOC	z/OS V2.3 Documentation Collection Hashsums for download (ftp://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/c27843007-CC_Eval.zip) SHA224: 84851b31fbf1bb4056944796b6f766c9d7ba1d36b4c26cf62d989c12 SHA256: 53d4a0ba82a3b67d031f3876fbceb88186b7d1ff2fe6af4ca6e8f7a7a422546d SHA384: d8d8b6c595d13ecb7a19f056395f62ea155a848c8f07a51d63ce812a7c485e73a9b83d26fee16cf67d6c452aaa794ef2 SHA512: 6c7207620867fc2d9ff80e72e31115a568c9606cf3b866a962739a297b32ab9206e4ead0bc2ebbb244f98c10b0cf906973b91		
4	DOC	ServerPac: IYO (Installing Your Order)	n/a	Hardcopy
5	DOC	Memo to Customers of z/OS V2.3 Common Criteria Evaluated Base	n/a	Hardcopy
6	DOC	z/OS V2.3 Planning for Multilevel Security and the Common Criteria; Document Number GA32-0891-30 SHA256 hashsum of the document:: 48cee926a44883fd7cb93b49e995b7f19f5da309b48a24aaef917a9738001b8f		
IBM Print Services Facility™ Version 4 Release 5 for z/OS (PSF V4.5.0, program number 5655-M32)				
7	SW	IBM Print Services Facility™ Version 4 Release 5 for z/OS (PSF V4.5.0, program number 5655-M32)	V4R5	Tape
8	DOC	Program Directory PSF V4.5 Base	GI13-3005-00	Hardcopy
OGL/370 V1.1.0 (program number 5688-191)				
9	SW	Overlay Generation Language Version 1 (OGL V1R1, program number 5688-191)	V1R1	Tape
10	DOC	OGL/370 V1.1.0: Getting Started	G544-3691-00	Hardcopy

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

No	Type	Identifier	Release	Form of Delivery
11	DOC	OGL/370 V1.1.0: LPS	G544-3697-00	Hardcopy
12	DOC	OGL: Command Summary and Quick Reference	S544-3703-01	Hardcopy
13	DOC	Program Directory OGL/370	GI10-0212-01	Hardcopy
Additional Media				
14	SW	PTFs for the following APARs (required): • OA52110 (PTF UA93049), • OA52192 (PTF UA93490), • OA52722 (PTF UA93924), • 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), These PTFs are to be obtained electronically from ShopzSeries (https://www.ibm.com/software/shopzseries)	n/a	Electronic

Tabella 4 – Materiali consegnabili dell'ODV

La consegna di tutti i materiali avviene in un unico pacchetto, prodotto appositamente per lo specifico cliente e spedito tramite corriere. Ulteriori aggiornamenti necessari devono quindi essere scaricati dal cliente tramite il sito Web ShopzSeries, seguendo le istruzioni fornite con il pacchetto.

Il download della guida dell'ODV (vedere l'articolo 3 nella precedente Tabella 4) è descritto in [MLSGUIDE]; in particolare, il cliente scarica la guida in formato elettronico da un server FTP IBM e quindi ne verifica la corrispondenza rispetto agli *hash* forniti in [MLSGUIDE].

La Tabella 4 contiene gli articoli che comprendono i diversi materiali dell'ODV, inclusi software e guida.

9.2 Identificazione dell'ODV

I materiali consegnati al cliente sono etichettati con gli identificativi di prodotto o documento e numero di versione come indicato in Tabella 4 e possono essere controllati dagli utenti che installano il sistema.

Il riferimento dell'ODV può essere verificato dall'amministratore durante il caricamento iniziale del programma (IPL), quando l'identificazione del sistema viene visualizzata sulla console di sistema. L'operatore può anche inserire il comando D IPLINFO, per visualizzare la versione di z/OS. La stringa "z/OS 02.03.00" deve essere visualizzata tra le altre informazioni.

9.3 Installazione, inizializzazione ed utilizzo sicuro dell'ODV

9.3.1 Installazione e configurazione del SW

L'elenco completo dei componenti SW da installare è riportato nella Tabella 4. Gli stessi elementi software sono utilizzati nelle modalità di sicurezza Labeled Security e Standard Mode, salvo quando diversamente indicato. La modalità operativa è definita dalla configurazione delle opzioni relative all'etichettatura in RACF. I dettagli sono descritti in z/OS Planning for Multilevel Security e Common Criteria ([MLSGUIDE]).

Le installazioni possono non utilizzare nessuno degli elementi forniti all'interno del ServerPac, ma è richiesto di installare, configurare ed utilizzare almeno i componenti RACF e ICSF dell'elemento z/OS Security Server.

Inoltre, software esterno all'ODV può essere aggiunto senza influire sulle caratteristiche di sicurezza del sistema, a patto che non sia eseguito in una delle seguenti modalità:

- in stato supervisor;
- come APF-authorized;
- con chiavi da 0 a 7;
- con UID(0);
- con autorità sulle risorse FACILITY BPX.DAEMON, BPX.SERVER o BPX.SUPERUSER;

- con autorità sulle 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;

- l'installazione di *system exit* eseguite in modalità autorizzata (stato supervisore, chiave di sistema o APF-authorized), ad eccezione del *sample* ICHPWX11 e della relativa routine IRRPHREX;

- installazione di plug-in IBM Tivoli Directory Server che non sono stati valutati;

- utilizzo della Authorized Caller Table (ICHAUTAB) in RACF per consentire ai programmi non autorizzati di inviare RACROUTE REQUEST = VERIFY (RACINIT) o RACROUTE REQUEST = LIST (RACLIST).

Nota*: la configurazione del software valutato non viene invalidata installando e facendo funzionare altri componenti adeguatamente certificati eventualmente eseguiti autorizzati. Tuttavia, la valutazione di tali componenti deve dimostrare che il componente e le politiche di sicurezza implementate dal componente non minino le politiche di sicurezza dell'ODV.*

Il componente IBM Tivoli Directory Server per z/OS può essere utilizzato come server LDAP, ma:

- Per l'autenticazione client tramite certificati digitali, l'amministratore deve configurare il server LDAP per mappare il certificato su un ID utente RACF e non eseguire il bind se il certificato non è mappato su un ID utente RACF. La configurazione LDAP consentita offre tre opzioni per formare un soggetto LDBM:

    - LDAP può utilizzare il DN originale dal certificato; o

    - LDAP può sostituire il DN originale con un DN in formato SDBM basato sull'ID utente RACF; o

    - LDAP può aggiungere il DN in formato SDBM all'argomento LDAP, dando un soggetto con due DN, uno dei quali funzionerà in ACL LDAP.

- L'autenticazione client mediante il meccanismo Kerberos non è stata valutata per LDAP e non può essere utilizzata nella configurazione valutata.

- L'autenticazione tramite password memorizzata in LDAP non può essere utilizzata. L'autenticazione deve avvenire utilizzando password RACF o password phrase. Da notare che se viene specificato un DN bind LDBM durante l'associazione al server, la password/phrase specificata deve essere per l'ID utente RACF associato a quel DN bind dall'amministratore LDAP;

- In modalità Labeled Security, è possibile utilizzare solo le configurazioni ICTX o LDBM. In modalità standard possono essere utilizzati i back-end LDBM, CDBM e SDBM e il plug-in ICTX. Altre configurazioni e plug-in di back-end LDAP non sono stati valutati e non devono essere utilizzati.

- (Solo modalità Labeled Security) Ogni istanza in esecuzione del server LDAP deve essere eseguita con una singola etichetta di sicurezza, non SYSMULTI, non SYSNONE. È possibile eseguire più istanze del server contemporaneamente, con etichette di sicurezza uguali o diverse.

Nella modalità Labeled Security, ogni istanza in esecuzione del server HTTP deve essere eseguita con un'etichetta di sicurezza che non sia né SYSMULTI né SYSNONE.

È possibile utilizzare il demone SSH sshd, ma se utilizzato:

- deve essere configurato per utilizzare il protocollo versione 2 e TDES o una delle suite di crittografia basate su AES,

- deve essere configurato in modalità di separazione privilegi e

- deve essere configurato per consentire solo l'autenticazione basata su password (inclusa password phrase) degli utenti o l'autenticazione basata su chiave pubblica degli utenti con le chiavi pubbliche memorizzate nei portachiavi RACF. L'autenticazione dell'utente basata su Rhost e su chiave pubblica con le chiavi archiviate altrove non può essere utilizzata nella configurazione valutata. In modalità Labeled Security, sshd deve essere configurato con l'etichetta di sicurezza SYSMULTI.

Il componente Network Authentication Service del componente Integrated Security Services, se utilizzato, e le applicazioni che lo sfruttano, devono soddisfare i seguenti vincoli:

- Il servizio di autenticazione di rete deve utilizzare il registro SAF (RACF). Il registro NDBM non è una configurazione valida per questa valutazione.

- Sono consentite le relazioni di trust incrociate con *realm* Kerberos esterni, ma il KDC esterno deve essere in grado di supportare la stessa cifratura del KDC z/OS.

- Al fine di garantire una forte protezione crittografica dei ticket Kerberos, Triple DES o AES dovrebbero essere utilizzati dal KDC z/OS e da qualsiasi KDC che partecipa a una relazione di trust tra regni e il KDC z/OS. DES dovrebbe essere utilizzato solo in ambienti di rete in cui la minaccia di attacchi crittografici contro i ticket e le sessioni protette da Kerberos è considerata sufficientemente bassa da giustificare l'uso di questi protocolli di crittografia più deboli.

- Le applicazioni che supportano Kerberos possono utilizzare una combinazione di protocolli specifici dell'applicazione e le funzioni GSS-API o i servizi richiamabili della piattaforma nativa equivalente (i servizi richiamabili SAF R_TicketServ e R_GenSec) per autenticare i client e nell'autenticazione client-server. Solo il meccanismo Kerberos può essere utilizzato da applicazioni che utilizzano GSS-API o le funzioni della piattaforma nativa equivalente. I servizi GSS-API e R_GenSec consentono anche la crittografia dei messaggi sensibili dell'applicazione passati tramite protocolli specifici dell'applicazione. Questi servizi consentono la comunicazione sicura tra applicazioni client e server. I servizi GSS-API includono l'integrità dei messaggi e le funzioni di privacy che convalidano l'autenticità e proteggono le comunicazioni tra client e server.

- È possibile utilizzare il server Network File System (NFS), ma deve essere configurato con l'opzione SAF o SAFEXPORT, per garantire che tutti gli accessi a file e directory (tranne possibilmente il montaggio di directory) siano sottoposti a controlli di sicurezza RACF appropriati.

TLS (Transport Layer Security):

- L'elaborazione TLS, se utilizzata, deve utilizzare i protocolli TLS V1.1 o TLS V1.2. TLS (Transport Layer Security), se utilizzato, deve utilizzare una delle suite di crittografia elencate nell'SFR FCS_COP.1 (NET) del TDS.

- Qualsiasi applicazione che esegue l'autenticazione client utilizzando 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 portachiavi che contengono la chiave privata dell'applicazione ed i certificati consentiti dall'autorità di certificazione (CA) che possono essere utilizzati per fornire i certificati client che l'applicazione supporterà. L'uso di gskkyman a 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 per le configurazioni valutate.

- Il server FTP di z/OS e il client possono supportare sia i protocolli del *draft* standard per la protezione FTP con TLS, sia i protocolli dal livello formale RFC 4217 di Security FTP con TLS [RFC4217]. Questa valutazione ha considerato solo il livello di supporto formale RFC 4217 e, di conseguenza, tale opzione deve essere utilizzata nella configurazione valutata.

- Le seguenti applicazioni non devono essere utilizzate nelle configurazioni Labeled Security, come indicato nella Guida alla configurazione IP di Communications Server: comando HOMETEST, IUCV, LPD, comando LPQ, comando LPR, comando LPRM, comando LPRSET, NCPROUTE, NPF, Portmapper, SMTP, Client NetView SNMP, comando client TELNET, comando TESTSITE, TNF, VMCF, subagente SLAPM2 di rete UNIX z/OS, subagente z/OS UNIX OMPROUTE SNMP, popper z/OS UNIX, agente z/OS UNIX RSVP, client SNMP z/OS UNIX comando, server e agente SNMP UNIX z/OS, demone Forwarder trap UNIX z/OS.

- L'elaborazione IPSec (IP Security), se utilizzata, deve utilizzare gli algoritmi di cifratura elencati nell'SFR FCS_COP.1 (NET).

RACF:

- Non utilizzare la funzione di condivisione remota RACF (RRSF) in modalità remota. Se si utilizza RRSF in modalità locale, assicurarsi che la direzione del comando non possa essere utilizzata eseguendo una delle seguenti operazioni:

- Assicurarsi che la classe RRFSFDATA non sia attiva.
- Definire il profilo DIRECT.* nella classe RRSFDATA con UACC (NONE) e nessun utente nell'elenco 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 che è consegnato con il prodotto che viene eseguito con i privilegi dell'utente deve essere usato con attenzione, poiché le TSF non possono proteggere quei client da programmi potenzialmente ostili. Le password/phrase che un utente inserisce in tali programmi client e che tali 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 i programmi client 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/phrase.

I seguenti elementi e componenti non possono essere utilizzati in un sistema valutato, perché violano le politiche di sicurezza indicate nel Traguardo di Sicurezza o perché sono stati rimossi dalla configurazione valutata a causa di vincoli di tempo e risorse della valutazione. Dato che 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.
- Server Infoprint.
- JES3.
- IBM Ported Tools per z/OS HTTP Server V7.0.

Inoltre, non è possibile utilizzare quanto segue nella configurazione certificata:

- Il componente Advanced Program to Program Program/Multiple Virtual Storage (APPC/MVS) del BCP.
- Il metodo di accesso agli oggetti DFSMS per le applicazioni con tipo content management.
- La funzione di condivisione remota RACF in modalità remota.
- Comunicazione JES2 NJE via TCP/IP. JES2 NJE deve utilizzare SNA o BSC nella configurazione certificata.
- Funzione JES2 Execution Batch Monitor (XBM).
- La maggior parte delle funzioni di Enterprise Identity Mapping (EIM). Per i dettagli, consultare il manuale [MLSGUIDE].

9.3.2 Installazione e configurazione dell'HW

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. Questa macchina astratta, che non fa parte dell'ODV, può essere fornita da uno dei seguenti sistemi:

- una partizione logica fornita da una versione certificata di PR/SM in esecuzione su:
    - IBM zEnterprise zEC12/BC12 con funzione di abilitazione DES/TDES CPACF 3863 attiva, con scheda Crypto Express3 o Crypto Express4S e con o senza l'estensione zEnterprise BladeCenter (zBX).
    - IBM z13/z13s con la funzione di abilitazione DES/TDES CPACF 3863 attiva, con schede Crypto Express4, Crypto Express4S o Crypto Express5S, con o senza l'estensione zEnterprise BladeCenter (zBX)[2].
    - IBM z14 con funzione di abilitazione DES/TDES CPACF 3863 attiva, con schede Crypto Express5S o Crypto Express6S.
- una versione certificata di IBM z/VM in esecuzione in una partizione logica fornita da PR/SM su uno dei processori System z™ sopra elencati.

[2] Se la configurazione include un'estensione zEnterprise BladeCenter (zBX), i sistemi operativi in esecuzione in zBX non fanno parte dell'ODV. Sono sistemi esterni, collegati a z/OS solo tramite le funzionalità di rete TCP/IP integrate incluse nel sistema zEnterprise e zBX.

10 Appendice B – Configurazione valutata

L'oggetto della valutazione è IBM z/OS Version 2 Release 3. L'ODV è solo software ed è accompagnato da documentazione guida. Gli elementi elencati nella Tabella 4 rappresentano l'ODV.

Il pacchetto base z/OS V2R3 valutato CC deve essere installato e configurato secondo le istruzioni fornite nel cap. 9.3.1 per la parte SW e come descritto nel cap. 9.3.2 per la parte 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 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 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 funzione di abilitazione DES/TDES CPACF 3863 attiva, con scheda Crypto Express3 o Crypto Express4S e con o senza l'estensione zEnterprise BladeCenter (zBX).
- IBM z13/z13s con la funzione di abilitazione DES/TDES CPACF 3863 attiva, con schede Crypto Express4, Crypto Express4S o Crypto Express5S, con o senza l'estensione zEnterprise BladeCenter (zBX).
- IBM z14 con funzione di abilitazione DES/TDES CPACF 3863 attiva, con schede Crypto Express5S o Crypto Express6S.

Si noti che le schede CryptoExpress 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.

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 traguardo di sicurezza [TDS], sezione 1.4.3.2.

I sistemi di test hanno eseguito z/OS Version 2 Release 3 nella configurazione valutata. A causa dell'enorme quantità di test, i test sono stati eseguiti durante lo sviluppo dell'ODV. Per garantire test adeguati di tutti i comportamenti rilevanti per la sicurezza dell'ODV, i Valutatori hanno verificato che tutti i test che potrebbero essere stati influenzati 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

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 macchina astratta che z/OS richiede per essere eseguita. Il test SAK è importante non solo per la valutazione z/OS, ma anche per altre valutazioni (PR/SM, z/VM).

L'FVT per z/OS viene in gran parte eseguito sul sistema di test VICOM. Questo è un sistema z/VM avanzato che implementa l'interfaccia macchina astratta z/Architecture. Consente ai tester 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. COMSEC è un ambiente che può essere gestito in modalità standard o con modalità Labeled Security. Il driver di test BERD (Background Environment Random Driver) invia i testcase come job JES2. L'orientamento di IBM è di spostare sempre più test in questo ambiente automatizzato, il che faciliterà sostanzialmente lo sforzo di test richiesto per le 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 3 nella configurazione valutata. 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.

L'approccio di test generale 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 persone viene dedicato a FVT e SVT per i componenti z/OS. FVT e SVT vengono eseguiti da team di test indipendenti, con tester indipendenti dagli Sviluppatori. 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 le singole funzioni di sicurezza dichiarate in [TDS] sono testate qui. 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 si è basata su tre cardini:

- La principale interfaccia di sicurezza interna è l'interfaccia con RACF, che è stata testata esaurientemente dal team di test 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 chiamano RACF, una volta che il test dell'interfaccia RACF ha verificato il corretto funzionamento interno di RACF.
- A causa della progettazione di z/OS, è visibile esternamente anche un gran numero di interfacce interne, 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 chiamanti non autorizzati.

Inoltre, 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

Lo Sviluppatore ha fornito una mappatura tra le TSF di [TDS], le TSFI nelle specifiche funzionali e i test eseguiti. Il Valutatore ha verificato questa mappatura ed esaminato i casi di test per verificare se i test riguardavano le funzioni e le loro interfacce. Sebbene non siano richiesti test approfonditi, il Committente ha fornito prove del fatto che sono stati testati dettagli significativi delle funzioni di sicurezza.

I Valutatori hanno stabilito che i test degli Sviluppatori hanno fornito 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 registri 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 le funzioni crittografiche è possibile accedere al supporto hardware fornito dall'ambiente IT dell'ODV 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, nonché sui sottosistemi che invocano RACF.

11.2.3 Risultati dei test

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

I Valutatori hanno verificato che i test sono stati eseguiti su configurazioni conformi al TDS, ad eccezione di alcune 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 di test basato sulle informazioni fornite dallo Sviluppatore.

Tramite questo ambiente di test, lo Sviluppatore è stato in grado di fornire ai Valutatori la prova della copertura necessaria e della profondità del test. Di fatto, IBM ha fornito ai Valutatori solo una parte dei loro test globali, per facilitare la gestione della complessità della valutazione.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

11.3.1 Approccio adottato per i test

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

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 che è stato impostato dai Valutatori secondo le specifiche trovate nella 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, consigliate dallo Sviluppatore per l'ODV, anche se non facevano parte della configurazione CC per i test. Tuttavia, come discusso in [ETR-TEST], il Valutatore ha fornito una spiegazione del perché questo è stato accettato.

11.3.2 Copertura dei test

Per i propri test, i Valutatori hanno deciso di concentrarsi sulle più importanti 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, per lo più impliciti, delle funzioni di identificazione e autenticazione in TSO/E, ftp e JES, dal momento che queste funzioni sono state ampiamente verificate durante l'attività di test da parte dei tester. I test dei tester si sono concentrati sui meccanismi di autenticazione basati su Kerberos e sulla gestione degli account TSO.
- Controllo d'accesso discrezionale: i Valutatori si sono concentrati sulla ACL dei servizi di sistema UNIX, che testano implicitamente anche i bit di autorizzazione UNIX. Altri test DAC coinvolti:
    - USS IPC (tutte le chiamate di sistema per messaggi, semafori e memoria condivisa).
    - DAC per diversi oggetti USS (file speciali del dispositivo, oggetti IPC, directory).
    - accesso al set di dati z/OS.
    - chiamate di sistema USS rilevanti per la sicurezza.
- Controllo di accesso obbligatorio: i Valutatori hanno rieseguito i propri test sulle verifiche del controllo di accesso obbligatorio per set di dati e file di Unix System Services come test di regressione. È stato inoltre eseguito il test della funzionalità di *writedown override* fornita dai profili di classe FACILITY.
- Sicurezza della comunicazione: i Valutatori hanno scelto di garantire che i canali di comunicazione sicuri (SSL, Kerberos e funzioni di rilevamento delle intrusioni) non contenessero errori nascosti di implementazione specifici della piattaforma testando l'interoperabilità con sistemi non zSeries. Application-transparent TLS (AT-TLS) è stato inoltre testato con una piattaforma non z/OS, controllando diverse impostazioni dei criteri.
- Audit: i test sono stati utilizzati per verificare l'auditing delle modifiche all'orologio di sistema.
- Gestione della sicurezza: i Valutatori hanno deciso di non elaborare test speciali in questo caso, poiché l'installazione dell'ambiente di test e il *setup/cleanup* dei test includevano già una parte importante delle TSF trovate.

- Autoprotezione dell'ODV: l'unica funzione opportunamente testabile è il riutilizzo degli oggetti. I Valutatori hanno deciso di concentrarsi sul problema delle pagine di memoria che probabilmente contenevano informazioni residue. Tutte le altre funzioni di autoprotezione sono proprietà che non potevano essere facilmente verificate dai test di valutazione.

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 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].

11.3.3 Risultati dei test

Tutti i casi di test elaborati 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 TDS.

11.4 Analisi delle vulnerabilità e test di intrusione

11.4.1 Approccio adottato per i test

Per quanto riguarda la valutazione della vulnerabilità, le modifiche introdotte in z/OS V2R3 rispetto alla versione precedente dell'ODV non hanno fornito ampie possibilità per ulteriori test di intrusione.

I test di intrusione del Valutatore hanno riguardato aree non prese in considerazione dalle precedenti valutazioni.

11.4.2 Copertura dei test

Il Valutatore ha verificato inizialmente la presenza della vulnerabilità indicata come CVE-2018-15473. Tuttavia, tale falla non è stata considerata problematica, in quanto non ha influenzato in modo significativo alcuna caratteristica di sicurezza dell'ODV o SFR.

La Tabella 5 riporta i test di intrusione che sono stati eseguiti.

USS Syscalls	*Effort*: The penetration testing examined the available system calls, supplying random arguments. No specific security function was subject to testing here. However, the system calls represent the full set of functions available to USS subjects. *Configuration*: The TOE was in its evaluated configuration. *Depth*: Any problem that would occur during testing, would potentially subvert the

	security functions behind that system call. The USS subsystem, as well as RACF are subject to testing here.
USS Stability	*Effort*: The penetration testing examined the USS subsystem's kernel with regard to resilience against random instruction streams. No specific security function was subject to testing here. *Configuration*: The TOE was in its evaluated configuration. *Depth*: The USS kernel the full set of functions available to USS subjects. Thus, any problem that would occur during testing, could potentially subvert the security functions the USS kernel controls. The USS subsystem, as well as RACF are subject to testing here.
TN3270 Control Character processing in program output	*Effort*: This is a classic penetration test, where irregular program output is not sanitized and the controlling terminal could be subverted. *Configuration*: The TOE was in its evaluated configuration. *Depth*: Any additional input from that terminal could then be used to subvert the system, thereby affecting all TSF. The system's console is one of the most privileged entry points into the system.

Tabella 5 – Test di intrusione

11.4.3 Risultati dei test

L'ODV è risultato resistente ai tentativi di intrusione in tutte le prove effettuate.

11.4.4 Vulnerabilità residue

I Valutatori hanno inoltre eseguito l'analisi delle vulnerabilità in base alle informazioni fornite nel TDS, alla documentazione di progettazione, alla rappresentazione dell'implementazione e alla guida per l'utente. Il Valutatore non ha rilevato alcuna nuova vulnerabilità introdotta da funzionalità nuove o modificate introdotte con z/OS V2R3 potenzialmente sfruttabile nell'ambiente operativo dell'ODV. Non è stata riscontrata alcuna vulnerabilità nelle fonti pubbliche verificate dal Valutatore (CVE e la mailing list RACF specifica per z/OS).

Il Valutatore ha analizzato in dettaglio le funzionalità di sicurezza aggiuntive che sono state recentemente introdotte o che sono state modificate in z/OS V2R3 per identificare potenziali vulnerabilità derivanti dalla progettazione e dall'implementazione di tali funzioni. Il Valutatore non ha identificato nessuna vulnerabilità sfruttabile nell'ambiente operativo previsto dell'ODV nell'ipotesi che il personale di amministrazione fidato osservi le linee guida per la configurazione e l'operatività dell'ODV.

Di seguito sono riepilogati le risultanze della valutazione precedente, che si applicano anche a z/OS V2R3:

- Controllando la progettazione e la documentazione di guida, il Valutatore ha rilevato che l'ODV è vulnerabile ad attacchi di Trojan Horse, virus, worm e attacchi analoghi in modo simile a quello di altri sistemi operativi. L'ODV non include funzionalità che contrastano tali attacchi in modo attivo. Sviluppare e lanciare con successo un tale attacco richiede la conoscenza dell'ODV e un potenziale di attacco superiore a quello identificato nel Traguardo di Sicurezza. Pertanto, tali vulnerabilità sono considerate non sfruttabili nell'ambiente previsto per l'ODV. Bisogna anche considerare che le ampie capacità di auditing dell'ODV consentono di identificare

un tale attacco, riducendo così la probabilità che tale attacco non venga rilevato in anticipo.

- Controllando la documentazione di progettazione, il Valutatore ha scoperto che la funzione di controllo di accesso obbligatoria dell'ODV non è progettata per evitare canali nascosti. Come nella maggior parte degli altri sistemi operativi sicuri multilivello, la sicurezza basata su etichette viene aggiunta a un sistema operativo che non è stato progettato pensando al controllo del flusso di informazioni. Di conseguenza, il Valutatore ha potuto riscontrare, come parte della sua analisi del progetto dell'ODV e dei documenti di guida, che l'ODV ha un numero considerevole di canali segreti (come tutti gli altri sistemi operativi sicuri multilivello in cui è stata aggiunta la Labeled Security), principalmente correlati ai blocchi di controllo del sistema e ad altri dati conservati in memoria comuni a tutti gli spazi degli indirizzi. Lo sfruttamento di un canale così nascosto richiede un programma Trojan Horse, che è stato valutato richiedere una conoscenza dell'ODV e un potenziale di attacco superiore a quello identificato nel Traguardo di Sicurezza. I canali segreti sono pertanto considerati una vulnerabilità residua non sfruttabile nell'ambiente previsto per l'ODV. Poiché i pacchetti di garanzia considerati in questa valutazione non richiedono un'analisi dei canali nascosti, il Valutatore non ha eseguito alcuna analisi per ottenere un elenco di canali nascosti, né un'analisi per determinare la loro larghezza di banda.

Le vulnerabilità residue riportate nella Tabella 6 sono presenti nell'ODV. Per ogni vulnerabilità si fornisce il calcolo del potenziale di attacco.

CVE-2018-0734	"The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p)." Assessment As indicated above, a timing side channel. This vulnerability is considered by OpenSSL to be of low severity, as it is difficult to exploit and no known exploits are present. This vulnerability is about recovering credentials of the OpenSSH host, therefore the SFRs that would be affected this are: FTP_ITC.1. As a side effect of this flaw, the contents of the host private key contained in a protected file would also be disseminated, which would subvert FDP_ACC.1(PSO) and FDP_ACF.1(TSO). However, as only the host key could be recovered mounting an attack impersonating the host would require additional network level subversions, such as taking over the host's ip address. The evaluator considered the CEM, appendix B 4.2 for calculating the attack potential here. *Elapsed Time*: The version of the OpenSSL library being used is not advertised, so the attacker needs some time to figure out the exact version that is being used in the TOE. Additionally, the attack programs need to be developed: Between one and two months. 5 points. *Expertise*: As no publicly available exploit is known, and the issue involves reconstructing private keys out of timing information, expert knowledge is needed.6 points. *Knowledge of the TOE*: Public knowledge of the TOE is sufficient. 0 points. *Window of Opportunity*: As the attack can only be mounted and more importantly developed with access to the TOE. A moderate window of opportunity is needed here. 4 points. *Equipment*: No exploit is known, therefore specialized slightly bespoke equipment is needed: 5 points *Summary*: 19 points, which would require an attack potential of "moderate".
CVE-2018-0735	"The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p)." Assessment As indicated above, a timing side channel. This vulnerability is considered by OpenSSL to be of low severity, as it is difficult to exploit and no known exploits are present. This vulnerability is about recovering credentials of the OpenSSH host, therefore the SFRs that would be affected this are: FTP_ITC.1. As a side effect of this flaw, the contents of the host private key contained in a protected file would also be disseminated, which would subvert FDP_ACC.1(PSO) and FDP_ACF.1(TSO). However, as only the host key could be recovered mounting an attack impersonating the host would require additional network level subversions, such as taking over the host's ip address. The evaluator considered the CEM, appendix B 4.2 for calculating the attack potential here. *Elapsed Time*: The version of the OpenSSL library being used is not advertised, so the attacker needs some time to figure out the exact version that is being used in the TOE. Additionally, the attack programs need to be developed: Between one and two months. 5 points. *Expertise*: As no publicly available exploit is known, and the issue involves reconstructing private keys out of timing information, expert knowledge is needed.6 points. *Knowledge of the TOE*: Public knowledge of the TOE is sufficient. 0 points. *Window of Opportunity*: As the attack can only be mounted and more importantly developed with access to the TOE. A moderate window of opportunity is needed here. 4 points. *Equipment*: No exploit is known, therefore specialized slightly bespoke equipment is needed: 5 points *Summary*: 19 points, which would require an attack potential of "moderate".

Tabella 6 – Vulnerabilità residue