Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

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

Certificato n. 10/22

(Certification No.)

Prodotto: IBM z/VM Version 7 Release 2 for VPP

(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:

Conforme a: Protection Profile for Virtualization, v1.0

(Conformant to)

(ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.1, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, AVA_VAN.1)

Il Direttore
(Dott.ssa Eva Spina)

Firmato digitalmente
da Eva Spina
Data: 2022.06.10
10:02:37 +02'00'

Roma, 10 giugno 2022

Common Criteria

Questa pagina è lasciata intenzionalmente vuota

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

IBM z/VM Version 7 Release 2 for VPP

OCSI/CERT/ATS/04/2021/RC

Versione 1.0

10 giugno 2022

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	10/06/2022

2 Indice

3 Elenco degli acronimi

APAR	Authorized Program Analysis Report
CAVS	Cryptographic Algorithm Validation System
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CMS	Conversational Monitor System
CP	Control Program
CPACF	CP Assist for Cryptographic Functions
CPU	Central Processing Unit
DAC	Discretionary Access Control
DASD	Direct Access Storage Device
DPCM	Decreto del Presidente del Consiglio dei Ministri
DVD	Digital Versatile Disk
EAL	Evaluation Assurance Level
I/O	Input/Output
ID	Identifier
IT	Information Technology
LGP	Linea Guida Provvisoria
LGR	Live Guest Relocation
LPAR	Logical Partition
LVS	Laboratorio per la Valutazione della Sicurezza
MFA	Multi-factor Authentication
NIAP	National Information Assurance Partnership
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

ODV	Oggetto della Valutazione
PP	Protection Profile
PR/SM	Processor Resource/System Manager
PTF	Program Temporary Fix
RACF	Resource Access Control Facility
RFV	Rapporto Finale di Valutazione
RNG	Random Number Generator
SAR	Security Assurance Requirement
SDF	Software Delivery and Fulfillment
SFR	Security Functional Requirement
SIE	Start Interpretive Execution
SSI	Single System Image
SSL	Secure Sockets Layer
ST	Security Target
TCP/IP	Transmission Control Protocol/Internet Protocol
TDS	Traguardo di Sicurezza
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

4 Riferimenti

4.1 Criteri e normative

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 4, September 2012

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 4, September 2012

[CC3] CCMB-2012-09-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 4, September 2012

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2012-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 4, September 2012

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

4.2 Documenti tecnici

[PP-VIRT] Protection Profile for Virtualization, pp_base_virtualization_v1.0, NIAP, Version 1.0, 17 November 2016

[PP-EPSV] Protection Profile for Virtualization Extended Package Server Virtualization, ep_sv_v1.0, NIAP, Version 1.0, 17 November 2016

[RC] “Rapporto di Certificazione IBM z/VM Version 7 Release 2”, OCSI/CERT/ATS/05/2020/RC, versione 1.0, 30 aprile 2021

[RFV] Final Evaluation Technical Report “IBM z/VM Version 7 Release 2”, OCSI-CERT-ATS-04-2021_ETR_220607_v2, Version 2, atsec information security GmbH, 7 June 2022

[TDS] “IBM z/VM Version 7 Release 2 for VPP Security Target”, Version 1.0, IBM Corporation, 16 may 2022

[ZVM-CPG] z/VM V7.2 Certified Product Guidance, IBM Corporation

[ZVM-SCG] z/VM V7.2 Secure Configuration Guide, SC24-6323-03, IBM Corporation, 12 May 2022

5 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La versione corrente dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

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

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

Il presente certificato è riconosciuto in ambito CCRA per tutti i componenti di garanzia dichiarati selezionati dai CC Parte 3 [CC3].

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "IBM z/VM Version 7 Release 2 for VPP", sviluppato da International Business Machines Corp. (IBM), nel seguito del documento anche indicato come z/VM V7R2 o z/VM.

L'ODV è un *hypervisor* di macchine virtuali per server mainframe IBM Z sui quali dislocare server virtuali per servizi critici.

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

Il presente Rapporto di Certificazione è stato emesso a conclusione della ri-certificazione dello stesso ODV (IBM z/VM Version 7 Release 2), già certificato dall'OCSI (Certificato n. 2/21 del 30 aprile 2021 [RC]).

Su richiesta del Fornitore IBM Corp., l'ODV è stato ri-certificato per soddisfare i requisiti del Protection Profile for Virtualization v1.0 [PP-VIRT] e del Server Virtualization Extended Package v1.0 [PP-EPSV] del NIAP. L'LVS atsec information security GmbH ha potuto riutilizzare parte della documentazione e delle evidenze già fornite nella precedente valutazione.

Pur rimanendo valide in gran parte le considerazioni e le raccomandazioni già espresse per il precedente ODV, per facilità di lettura il presente Rapporto di Certificazione è stato riscritto nella sua interezza in modo da costituire un documento autonomo associato al nuovo ODV "IBM z/VM Version 7 Release 2 for VPP".

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 i componenti di garanzia inclusi nel PP [PP-VIRT], 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/VM Version 7 Release 2 for VPP" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti e/o utilizzatori per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

Il presente Rapporto di Certificazione deve essere consultato congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	IBM z/VM Version 7 Release 2 for VPP
Traguardo di Sicurezza	"IBM z/VM Version 7 Release 2 for VPP Security Target", Version 1.0 [TDS]
Livello di garanzia	Conforme a PP con i seguenti componenti di garanzia: ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.1, ASE_SPD.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1 e AVA_VAN.1
Fornitore	IBM Corporation
Committente	IBM Corporation
LVS	atsec information security GmbH
Versione dei CC	3.1 Rev. 4
Conformità a PP	Protection Profile for Virtualization v1.0 [PP-VIRT] col seguente Extended Package: • Protection Profile for Virtualization Extended Package Server Virtualization v1.0 [PP-EPSV]
Data di inizio della valutazione	21 giugno 2021
Data di fine della valutazione	7 giugno 2022

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

7.3 Prodotto valutato

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

L'ODV è il prodotto z/VM Version 7 Release 2 configurato in un cluster comprendente fino a quattro istanze di z/VM in collaborazione all'interno di una Single System Image (SSI).

z/VM è un sistema operativo estremamente sicuro, flessibile, robusto e scalabile che implementa un *hypervisor* di macchine virtuali per i server mainframe IBM Z sui quali dislocare server virtuali per servizi critici. z/VM è progettato per ospitare altri sistemi operativi, ciascuno nella propria macchina virtuale.

Più macchine virtuali possono essere eseguite contemporaneamente per svolgere una varietà di funzioni che richiedono accesso controllato e separato alle informazioni memorizzate nel sistema. Oltre ai server virtuali, l'ODV fornisce macchine virtuali aggiuntive per ciascun utente umano connesso, separando il dominio di esecuzione di ogni macchina virtuale dagli altri, secondo quanto stabilito nelle definizioni della macchina virtuale memorizzate nella directory di sistema. In aggiunta a questo meccanismo, l'accesso a risorse e funzioni privilegiate viene mediato dal server di sicurezza RACF.

L'ODV offre una tecnologia di *clustering* multi-sistema che consente di avere da una a quattro istanze di z/VM in un cluster SSI. La configurazione del cluster, così come il suo stato, sono conservati in risorse condivise tra i membri del cluster. Nuove istanze di z/VM possono essere aggiunte alla topologia del cluster in fase di *runtime*. Il supporto per Live Guest Relocation (LGR) consente lo spostamento dei server virtuali Linux senza interruzione della loro operatività. I membri del cluster sono a conoscenza l'uno dell'altro e possono trarre vantaggio dalle loro risorse combinate. LGR consente di evitare interruzioni del servizio dei client in caso di manutenzioni pianificate spostando gli *host* da un sistema che richiede interruzione ad un sistema che invece rimane attivo durante il periodo di manutenzione.

Il database RACF utilizzato per preservare il contesto di sicurezza dell'ODV è condiviso tra i membri del cluster. Tutti i membri del cluster eseguono un'istanza separata di RACF per l'audit locale, con accesso al database RACF condiviso.

Il concetto di macchine virtuali che rappresentano utenti gestiti da una singola istanza di z/VM può essere esteso fino a corrispondere ad una topologia cluster. Una macchina virtuale configurata come USER può essere eseguita in un dato momento soltanto su uno dei membri del cluster, mentre le macchine virtuali a configurazione multipla, configurate come IDENTITY, possono essere eseguite simultaneamente su diversi membri del cluster e rappresentano generalmente macchine di servizio.

z/VM fornisce identificazione e autenticazione degli utenti, controllo di accesso discrezionale (DAC) ad un gran numero di oggetti diversi, separazione delle macchine virtuali, funzionalità di audit configurabile, funzioni di gestione della sicurezza avanzate, preparazione degli oggetti per il riutilizzo e funzionalità interne per la protezione da interferenze e manomissioni da parte di utenti o soggetti non attendibili.

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

7.3.1 Architettura dell'ODV

7.3.1.1 Panoramica generale dell'ODV

L'ODV è il prodotto di tipo *hypervisor* z/VM, configurato come parte di un cluster SSI formato da una o più istanze di z/VM, che include i componenti software descritti nel capitolo 1.5.4 del Traguardo di Sicurezza [TDS].

z/VM è un sistema operativo progettato per ospitare altri sistemi operativi, ciascuno all'interno della propria macchina virtuale. Più macchine virtuali possono essere eseguite contemporaneamente per espletare una varietà di funzioni che richiedono accesso controllato e separato alle informazioni memorizzate nel sistema. L'ODV fornisce una macchina virtuale per ciascun utente che ha effettuato l'accesso, separando il dominio di esecuzione di ciascun utente da altri utenti, secondo quanto stabilito nelle definizioni della macchina virtuale memorizzate nella directory di sistema. Inoltre, la directory di sistema contiene informazioni relative al controllo di accesso alle funzioni privilegiate, come ad esempio l'utilizzo di alcune opzioni dell'istruzione DIAGNOSE del processore. In aggiunta a questo meccanismo, l'accesso a risorse e funzioni privilegiate viene mediato dal server di sicurezza RACF.

L'ODV è visto come un'istanza di un cluster SSI che comprende da uno a quattro sistemi z/VM individuali. Questi singoli sistemi z/VM vengono eseguiti ciascuno all'interno di una macchina astratta come unico sistema operativo a livello della macchina astratta stessa ed esercitano il pieno controllo su di essa, indipendentemente dal software in esecuzione all'interno delle macchine virtuali. Queste macchine astratte sono fornite da partizioni logiche (LPAR) dei server mainframe IBM.

Le LPAR non fanno parte dell'ODV, ma appartengono all'ambiente operativo. Si noti che, sebbene un'istanza di z/VM possa essere eseguita all'interno di un'altra istanza di z/VM, la configurazione valutata è limitata ad un'istanza di z/VM in esecuzione direttamente all'interno di una LPAR. Un'istanza di z/VM in esecuzione all'interno di una macchina virtuale è consentita, ma tali istanze di z/VM di "secondo livello" non fanno parte della configurazione valutata.

La funzione SSI di z/VM consente di configurare fino a quattro sistemi z/VM come membri di un cluster SSI, che condividono risorse diverse.

I membri del cluster SSI possono trovarsi sullo stesso apparato hardware o su apparati separati. SSI consente di gestire i membri del cluster come un unico sistema, il che consente di effettuare la manutenzione di ciascun membro del cluster senza dover interrompere l'operatività dell'intero cluster. SSI implementa anche il concetto di Live Guest Relocation (LGR) grazie al quale un sistema operativo Linux in esecuzione può essere spostato da un membro di un cluster ad un altro senza che sia necessario arrestarlo completamente durante il processo di trasferimento.

Tutte le istanze di z/VM membri di un cluster SSI condividono il database RACF, ma non condividono i dischi di audit di RACF. Ogni istanza di z/VM deve eseguire la propria istanza di RACF, la quale accede al database RACF condiviso. La condivisione del database RACF avviene condividendo tra le diverse istanze di z/VM del cluster SSI il volume DASD (Direct Access Storage Device) in cui è memorizzato il database RACF. Sebbene sia tecnicamente possibile condividere il database RACF tra z/VM e z/OS, questa possibilità è esplicitamente esclusa dalla valutazione.

Il database RACF può anche essere condiviso da diverse istanze dell'ODV. La condivisione è implementata in maniera simile alla condivisione del database RACF all'interno del cluster SSI. Tuttavia, a seconda dello scenario di utilizzo, tale condivisione potrebbe non essere consigliabile.

Le piattaforme hardware selezionate per la valutazione sono costituite da prodotti IBM che risultano disponibili alla data di chiusura della valutazione e che rimarranno disponibili anche in seguito per un certo periodo di tempo. Un prodotto eventualmente ritirato dal mercato può comunque essere ottenuto tramite richiesta speciale a IBM.

Le funzioni di sicurezza dell'ODV (TSF) sono fornite dal *kernel* del sistema operativo z/VM, denominato Control Program (CP), e dall'applicazione RACF in esecuzione all'interno di una macchina virtuale con privilegi speciali. Oltre a fornire i servizi di autenticazione dell'utente, di controllo di accesso e di audit al CP, RACF può fornire gli stessi servizi ad altre macchine virtuali autorizzate. z/VM fornisce funzioni di gestione che consentono di configurare il TSF adattandolo alle esigenze del cliente.

L'ODV include alcuni elementi che non forniscono funzionalità di sicurezza, ma vengono eseguiti in modalità autorizzata e potrebbero quindi, in caso di comportamento anomalo, compromettere l'ODV. Poiché questi elementi sono importanti per l'operatività degli ambienti di molti utilizzatori finali, sono stati inclusi all'interno dell'ODV sotto forma di applicazioni attendibili.

7.3.1.2 Principali componenti software dell'ODV

L'ODV è costituito da un massimo di quattro istanze di z/VM, ciascuna definita da tre componenti principali: il Control Program (CP), il Security Manager RACF e il componente TCP/IP. RACF e TCP/IP vengono eseguiti all'interno di macchine virtuali dedicate gestite dal CP.

Il CP di z/VM è principalmente un gestore di risorse di macchine reali. Il CP fornisce a ciascun utente un ambiente di lavoro individuale noto come macchina virtuale. Ogni macchina virtuale è l'equivalente funzionale di un sistema fisico e sfrutta in condivisione le istruzioni e le funzionalità del processore reale, le memorie, la console e le risorse dei dispositivi di I/O.

Il CP fornisce il supporto alla connettività che consente ai programmi applicativi in esecuzione all'interno di macchine virtuali di scambiarsi informazioni tra loro e di accedere alle risorse che risiedono sullo stesso sistema z/VM o su sistemi z/VM diversi.

Allo scopo di creare e mantenere queste regole (definizioni delle macchine virtuali) vengono utilizzati software aggiuntivi di gestione, che vengono eseguiti esternamente al CP ma che fanno comunque parte dell'ODV. Per questo motivo, ogni componente del software di gestione viene eseguito all'interno di una macchina virtuale. Di seguito sono elencate le funzionalità eseguite all'interno di macchine virtuali:

- **CMS**: un sistema operativo multiuso per utente singolo utilizzato per eseguire le applicazioni RACF e TCP/IP. CMS non fornisce alcuna funzionalità di sicurezza ma implementa un *file system* che può essere utilizzato dalle applicazioni in esecuzione.

- **Server RACF**: fornisce servizi di autenticazione, autorizzazione e audit al CP e ad altre macchine virtuali autorizzate che eseguono applicazioni su CMS. Viene eseguito all'interno di una macchina virtuale gestita dal CP e comunica col CP attraverso un'interfaccia ben definita strettamente controllata.

- **Server TCP/IP**: fornisce i tradizionali servizi di comunicazione basati su IP. Per le comunicazioni cifrate TLS interagisce con il server SSL, che viene visto come un sotto-componente del componente TCP/IP piuttosto che come una porzione aggiuntiva dell'ODV. Il server TCP/IP e il server SSL non fanno parte del CP, ma vengono eseguiti ognuno all'interno di una rispettiva macchina virtuale gestita dal CP.

Incorporato nello *stack* TCP/IP si trova il servizio Telnet, che consente agli utenti di accedere alle console delle loro macchine virtuali ("log on") dalla rete IP. In particolare, il servizio Telnet riceve il traffico della console dalla rete, rimuove l'incapsulamento dei protocolli Telnet o TN3270 e lo inoltra al CP utilizzando una forma speciale dell'istruzione DIAGNOSE del processore. Il CP genera una sessione di console virtuale come oggetto in memoria. Tutte le informazioni in uscita vengono restituite dal CP al servizio Telnet, che le incapsula nel protocollo Telnet o TN3270E e le invia al client. Il server TCP/IP fornisce anche servizi TLS che consentono la creazione di un canale di comunicazione protetto da cifratura.

7.3.2 Caratteristiche di sicurezza dell'ODV

Il problema di sicurezza dell'ODV, comprendente obiettivi di sicurezza, ipotesi, minacce e politiche di sicurezza dell'organizzazione, è definito nel cap. 3 del Traguardo di Sicurezza [TDS].

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

- **Identificazione e autenticazione**: l'ODV fornisce la funzionalità di identificazione e autenticazione degli utenti mediante un ID utente alfanumerico ed una password mantenuta cifrata dal sistema. I seguenti componenti dell'ODV eseguono l'identificazione e l'autenticazione in maniera indipendente:

    - Control Program (CP)

    - RACF

  A supporto di identificazione e autenticazione, l'ODV utilizza RACF per gestire i profili di risorse e i profili utente. Le decisioni basate sull'autenticazione a più fattori possono anche essere affidate a un provider MFA esterno, se configurato. Tali decisioni basate su MFA vengono successivamente applicate dall'ODV.

- **Controllo di accesso discrezionale (DAC)**: per l'implementazione di regole DAC estese viene utilizzato il componente dell'ODV RACF, che offre la funzionalità e la flessibilità richieste dal livello di valutazione in confronto all'utilizzo del sistema. In sostanza, in un sistema protetto da RACF l'autorizzazione dell'utente ad accedere ad una risorsa in un qualsiasi momento è determinata da una combinazione dei seguenti fattori:

- identità dell'utente e gruppo di appartenenza;
- attributi dell'utente, inclusi gli attributi a livello di gruppo;
- autorità del gruppo dell'utente;
- autorità di accesso specificata nel profilo della risorsa.

- **Separazione delle macchine virtuali**: eventuali malfunzionamenti del sistema operativo che si verificano all'interno delle macchine virtuali non possono influire sull'ODV in esecuzione sul processore reale. Poiché l'errore viene isolato sulla macchina virtuale, solo quella macchina virtuale si interrompe e può essere riavviata senza influire negativamente sui processi in esecuzione su altre macchine virtuali. In particolare, i server virtuali critici non sono interessati dai guasti delle macchine virtuali associate agli utenti umani che hanno effettuato l'accesso.
  Tramite il supporto del processore sottostante, l'ODV circoscrive le conseguenze di errori software (come interrupt di programma causati da eccezioni intercettate) che si verificano in una macchina virtuale a quella specifica macchina, non influenzando quindi altre macchine virtuali o il CP.
  Errori del CP che non possono essere isolati su una delle macchine virtuali gestite comportano la terminazione anomala ("abnormal end", abbreviato in *abend*) del CP stesso. In caso di *abend*, il sistema si reinizializzerà da solo, se possibile. Alle condizioni di *abend* sono associati codici numerici speciali che ne identificano la causa.

- **Audit**: l'ODV fornisce una funzionalità di audit che consente di generare record di audit per eventi critici di sicurezza. RACF offre una serie di funzioni di log e reportistica che consentono agli utenti proprietari delle risorse e agli utenti con ruolo auditor di identificare gli utenti che tentano di accedere alle risorse. I record di audit generati da RACF vengono memorizzati in file residenti su dischi protetti da modifiche o cancellazioni non autorizzate dal meccanismo DAC.
  I record di audit relativi alle connessioni TLS sono generati dal server TLS e vengono raccolti da utenti privilegiati che accedono al comando SSLADMIN. Questi record di audit sono protetti da modifiche o cancellazioni non autorizzate dal meccanismo DAC.

- **Riutilizzo degli oggetti**: l'ODV fornisce una funzione che cancella gli oggetti protetti e gli spazi di archiviazione precedentemente utilizzati dalle macchine virtuali o dall'ODV stesso prima della riassegnazione ad altre macchine virtuali o all'ODV. Ciò garantisce la riservatezza dei dati gestiti dall'ODV e dalle macchine virtuali.
  I dispositivi DASD e i loro derivati (come minidischi o dischi temporanei) devono essere cancellati manualmente dall'amministratore in conformità con le politiche dell'organizzazione. Supporto aggiuntivo è fornito dal software IBM Directory Maintenance Facility (DirMaint), che tuttavia non fa parte della valutazione.

- **Gestione della sicurezza**: l'ODV fornisce una serie di comandi e opzioni per gestire in modo adeguato le funzioni di sicurezza. L'ODV definisce diversi ruoli che sono autorizzati ad eseguire le diverse attività di gestione relative alla sicurezza dell'ODV:

- Le opzioni di sicurezza generali sono gestite dagli amministratori della sicurezza.
- La gestione degli utenti e dei relativi attributi di sicurezza viene eseguita dagli amministratori della sicurezza. La gestione dei gruppi può essere delegata ad amministratori della sicurezza dei gruppi.
- La gestione delle definizioni delle macchine virtuali viene eseguita dagli amministratori della sicurezza.
- Gli utenti possono modificare la propria password, il loro gruppo predefinito e il loro nome utente.
- Gli auditor gestiscono i parametri del sistema di audit (ad esempio l'elenco degli eventi controllati) e possono analizzare l'*audit trail*.

- **Protezione del TSF**: il CP dell'ODV garantisce l'integrità del proprio dominio. Nessuna macchina virtuale può accedere alle risorse dell'ODV senza un'autorizzazione appropriata. Ciò impedisce la manomissione delle risorse dell'ODV da parte di soggetti non attendibili.
  A supporto di questa funzionalità vi sono caratteristiche implementate in hardware, in particolare la Interpretive-Execution Facility (istruzione SIE). Pertanto, i componenti hardware e firmware che forniscono la macchina astratta per l'ODV devono essere protetti fisicamente da accessi non autorizzati.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto, viene fornita al cliente insieme al prodotto.

La documentazione indicata contiene le informazioni richieste per l'inizializzazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel par. 8.3 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] dichiara conformità *exact* ai seguenti Profili di Protezione e pacchetti estesi:

- Protection Profile for Virtualization, Version 1.0 [PP-VIRT]
- Protection Profile for Virtualization Extended Package Server Virtualization, Version 1.0 [PP-EPSV]

7.6 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati o ricavati per estensione dai CC Parte 3 [CC3].

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

Considerando che il TDS dichiara conformità *exact* al Protection Profile for Virtualization [PP-VIRT] e al Server Virtualization Extended Package [PP-EPSV], sono inclusi tutti e soli i SAR e gli SFR definiti in questo PP e nel relativo EP.

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

7.7 Conduzione della valutazione

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

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM]. Inoltre, sono state eseguite tutte le attività di garanzia specifiche richieste dal Protection Profile for Virtualization [PP-VIRT] e dal Server Virtualization Extended Package [PP-EPSV].

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 7 giugno 2022 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione l'8 giugno 2022. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 Considerazioni generali sulla validità della certificazione

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

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale

insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

8 Esito della valutazione

8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV] prodotto dall'LVS atsec information security GmbH e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "IBM z/VM Version 7 Release 2 for VPP" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia definito dai SAR inclusi nel PP [PP-VIRT], in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B – Configurazione valutata.

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia definito dai SAR inclusi nel PP [PP-VIRT].

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
Stated security requirements	ASE_REQ.1	Positivo
Security problem definition	ASE_SPD.1	Positivo
TOE summary specification	ASE_TSS.1	Positivo
Development	**Classe ADV**	Positivo
Basic functional specification	ADV_FSP.1	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
Labelling of the TOE	ALC_CMC.1	Positivo
TOE CM coverage	ALC_CMS.1	Positivo
Timely Security Updates	*ALC_TSU_EXT.1*	Positivo
Test	**Classe ATE**	Positivo
Independent testing - conformance	ATE_IND.1	Positivo
Vulnerability assessment	**Classe AVA**	Positivo

Classi e componenti di garanzia		Verdetto
Vulnerability survey	AVA_VAN.1	Positivo

Tabella 1 - Verdetti finali per i requisiti di garanzia

8.2 Attività di garanzia aggiuntive

Il Protection Profile for Virtualization [PP-VIRT] e il Server Virtualization Extended Package [PP-EPSV] includono attività di garanzia aggiuntive che sono specifiche per il tipo di tecnologia dell'ODV e sono richieste per la conformità *exact* al PP e all'EP.

I Valutatori hanno utilizzato per le attività di garanzia del PP/EP una notazione simile a quella dei componenti delle classi di garanzia CC esistenti. L'obiettivo di queste sotto-attività è quello di determinare se sono soddisfatti tutti i requisiti delle attività di garanzia incluse nel PP/EP.

La Tabella 2 riassume i verdetti finali di ciascuna attività di garanzia del PP/EP svolta dall'LVS.

Attività di garanzia del PP/EP		Verdetto
ASE: Security Target evaluation	ASE_BVPP.1	Positivo
	ASE_SVEP.1	Positivo
AGD: Guidance documents	AGD_BVPP.1	Positivo
	AGD_SVEP.1	Positivo
ALC: Life cycle support	ALC_BVPP.1	Positivo
ATE: Tests	ATE_BVPP.1	Positivo
	ATE_SVEP.1	Positivo

Tabella 2 - Verdetti finali per le attività di garanzia del PP/EP

8.3 Raccomandazioni

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

Si raccomanda ai potenziali acquirenti del prodotto "IBM z/VM Version 7 Release 2 for VPP" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo agli Obiettivi di Sicurezza per l'ambiente operativo specificati nel par. 4.2 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le ipotesi descritte nel par. 3.2 del Traguardo di Sicurezza [TDS].

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 ([ZVM-CPG], [ZVM-SCG]).

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

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

9.1 Consegna dell'ODV

L'ODV è composto unicamente da software; nessun componente hardware o firmware viene fornito come parte del prodotto.

In Tabella 3 sono elencati gli elementi che costituiscono l'ODV, inclusi il software e i documenti di guida.

#	Tipo	Identificativo	Release	Metodo di consegna
z/VM Version 7 Release 2.0				
1	SW	z/VM Version 7 Release 2, program number 5741-A09	V7R2	DVD / Download
2	DOC	Program Directory for z/VM V7R2 Base	GI13-4358-01	Copia cartacea
3	DOC	Program Directory for RACF function level 720	GI13-4364-01	Copia cartacea
4	DOC	Guide for Automated Installation and Service	GC24-6292-02	Copia cartacea
5	DOC	z/VM V7.2 Certified Product Guidance sha256-Checksum: 923da02dad4aa9bbc6c4a19ed565eac364f53914496578c0332c464078b56504 2022 May Refresh zVM720 Collection.zip	n/a	Copia elettronica
6	DOC	z/VM V7.2 Secure Configuration Guide for VPP sha256-Checksum: 21d55f6060b6f81b029143a2ddc203858906b1fadc6f42ccc91d1e78c764cfef hcps0_v7r2.pdf	SC24-6323-03	Copia elettronica
Elementi aggiuntivi				
7	SW	RSU1 (the z/VM 7.2 GA level of service) to be obtained electronically from IBM Shopz	n/d	Download
8	SW	PTF for APAR PH24751 to be obtained electronically from IBM Shopz	n/d	Download
9	SW	PTF for APAR VM66540 to be obtained electronically from IBM Shopz	n/d	Download
10	SW	PTF for APAR PH28216 to be obtained electronically from IBM Shopz	n/d	Download

Tabella 3 - Elementi consegnabili dell'ODV

I clienti in possesso di un ID cliente IBM appropriato possono utilizzare il portale Web IBM Shopz (https://www.ibm.com/software/shopzseries/ShopzSeries_public.wss) per effettuare l'ordine dell'ODV. Nel caso in cui il cliente necessiti di assistenza, può contattare un rappresentante di vendita IBM che supporterà il cliente nella compilazione del modulo d'ordine.

Gli ordini del prodotto z/VM vengono elaborati da un Centro di Produzione SDF. Il file immagine di z/VM viene duplicato su un set di supporti DVD, che viene quindi imballato in una scatola di cartone e sigillato con pellicola termoretraibile. Il pacco finale viene quindi consegnato al cliente assieme alla lista del contenuto tramite un servizio di corriere.

L'intero processo che va dalla preparazione ed etichettatura dei supporti alla consegna finale del pacco sigillato al cliente, avviene sotto la supervisione di un sistema di controllo che utilizza un sistema di identificazione basato su codici a barre per tutte le parti di un ordine, fino al completamento del processo. Il codice a barre consente l'associazione univoca dei supporti e della documentazione aggiuntiva ad un numero d'ordine specifico e, quindi, al cliente che ha effettuato l'ordine corrispondente.

Una volta che il pacco è stato consegnato presso il luogo specificato nell'ordine, il cliente è in grado di verificarne la corrispondenza con quanto ordinato effettuando un controllo incrociato tra i codici prodotto riportati nella lista del contenuto inclusa nella consegna e quelli stampati sulle etichette dei supporti consegnati.

9.2 Identificazione dell'ODV

Durante il processo di ordine dell'ODV, il cliente deve richiedere esplicitamente la versione certificata CC di z/VM Versione 7 Release 2. Questo fornisce già la garanzia il prodotto consegnato al cliente è effettivamente l'ODV comprensivo di tutti i componenti necessari. Dopo aver effettuato l'installazione del prodotto secondo quanto indicato nel documento Secure Configuration Guide [ZVM-SCG], l'amministratore sarà in grado di verificare la versione dell'ODV mediante il comando:

```
QUERY CPLEVEL
```

Questo commando dovrà restituire a schermo la seguente stringa di versione:

```
z/VM Version 7 Release 2.0, service level 2001 (64-bit)
```

L'amministratore dovrà inoltre verificare l'elenco delle PTF installate confrontandolo con quello delle PTF richieste indicato nel Traguardo di Sicurezza [TDS]. A tale scopo, l'amministratore potrà utilizzare i comandi seguenti:

```
VMFSIM QUERY 7VMCPR20 SRVAPPS * TDATA :PTF
VMFSIM QUERY 7VMRAC20 SRVAPPS * TDATA :PTF
VMFSIM QUERY 7VMTCP20 SRVAPPS * TDATA :PTF
```

Questi comandi dovranno restituire in output le PTF indicate nel seguito.

Per il CP dovranno risultare installate le seguenti PTF:

```
UM35699
UMRSU01
```

Per il componente TCP/IP dovrà risultare installata la seguente PTF:

```
UI72767
UI72963
```

Per RACF non dovrà risultare installata nessuna PTF.

9.3 Installazione, inizializzazione e utilizzo sicuro dell'ODV

L'installazione, la configurazione e l'operatività dell'ODV devono essere eseguite secondo le istruzioni riportate nelle sezioni appropriate della documentazione di guida fornita con il prodotto al cliente.

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

- z/VM V7.2 Secure Configuration Guide [ZVM-SCG]
- z/VM V7.2 Certified Product Guidance [ZVM-CPG]

La Secure Configuration Guide contiene riferimenti ad altra documentazione di guida pertinente contenuta nella Certified Product Guidance di z/VM. Sia la Secure Configuration Guide, sia la Certified Product Guidance sono disponibili per il download sicuro al seguente ResourceLink sul sito Web di IBM:

```
https://www.ibm.com/servers/resourcelink/svc0302a.nsf/pages/zVMV7R2Library
```

La documentazione è altresì disponibile nelle rispettive sezioni della libreria IBM z/VM 7.2 accessibile al seguente link:

```
https://www.vm.ibm.com/library/index.html
```

10 Appendice B – Configurazione valutata

L'oggetto di valutazione (ODV) è il prodotto "IBM z/VM Version 7 Release 2 for VPP", sviluppato dalla società IBM Corp. L'ODV è composto unicamente da software ed è accompagnato dalla documentazione di guida. L'ODV è rappresentato dagli elementi elencati in Tabella 3.

L'ODV è rappresentato da un cluster SSI composto da un massimo di quattro istanze in collaborazione del prodotto z/VM, ciascuna in esecuzione su una macchina astratta. Ogni istanza di z/VM è installata come unico sistema operativo a livello della macchina astratta ed esercita il controllo completo sulla macchina astratta, indipendentemente dal software in esecuzione all'interno delle macchine virtuali. Le macchine astratte sono fornite da una versione certificata di PR/SM sul seguente processore IBM z System, come indicato nel par. 1.5.4.4 del Traguardo di Sicurezza [TDS]:

- IBM Z z14 con attiva la CPACF Enablement Feature 3863

Le LPAR non fanno parte dell'ODV, ma appartengono all'ambiente operativo dell'ODV. Si noti che, sebbene un'istanza di z/VM possa tecnicamente essere eseguita all'interno di un'altra istanza z/VM, la configurazione valutata è limitata ad istanze di z/VM eseguite direttamente all'interno di una LPAR. Un'istanza di z/VM in esecuzione all'interno di una macchina virtuale è consentita, ma tali istanze di z/VM di "secondo livello" non fanno parte della configurazione valutata.

La configurazione valutata dell'ODV è inoltre definita dai requisiti di configurazione che devono essere soddisfatti, come indicato nel documento Secure Configuration Guide [ZVM-SCG] che fa parte dei materiali consegnabili dell'ODV.

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 definito dai SAR inclusi nel PP [PP-VIRT], tali attività non prevedono l'esecuzione di test funzionali da parte del Fornitore, ma soltanto test funzionali indipendenti e test di intrusione da parte dei Valutatori.

11.1 Configurazione per i Test

I test del Fornitore e i test indipendenti dei Valutatori sono stati eseguiti sulla stessa configurazione, vale a dire sui due sistemi di test denominati GDLMCCC e GDLPCCC, ciascuno in esecuzione all'interno di una partizione logica separata.

Le partizioni logiche sono state fornite da versioni certificate di PR/SM su un server IBM z14 (GDLPCCC) e su un server IBM z15 (GDLMCCC). In considerazione del fatto che in un cluster SSI tutti i membri sono limitati a un livello di funzionalità di CPU comune, vale a dire z14 nel caso in esame, i server utilizzati per i test risultano congruenti con l'elenco di piattaforme hardware supportate riportato nel par. 1.5.4.4 del Traguardo di Sicurezza [TDS].

Sia per le sessioni di test del Fornitore, sia per quelle dei Valutatori, l'ODV è stato installato sui sistemi di test nella sua configurazione valutata, così come richiesto dal Traguardo di Sicurezza [TDS]. Ciò è stato confermato dai Valutatori, che hanno analizzato le evidenze generate dal Fornitore ed eseguito controlli aggiuntivi durante la preparazione e l'esecuzione dei test indipendenti.

11.2 Test funzionali ed indipendenti svolti dai Valutatori

I Valutatori hanno eseguito due tipologie di test: i test indipendenti, come definiti nel Protection Profile for Virtualization [PP-VIRT] e nel Server Virtualization Extended Package [PP-EPSV], e i test CAVS degli algoritmi crittografici.

I Valutatori hanno eseguito tutti i test definiti nel PP [PP-VIRT] e nell'EP [PP-EPSV], che ammontano a circa 100 casi di test. Per quanto riguarda i requisiti di test per le primitive crittografiche e per l'algoritmo RNG, sono stati eseguiti i test CAVS su tutti gli algoritmi crittografici applicabili. I test dei Valutatori sono stati effettuati in parte manualmente e in parte in modalità automatica.

I test indipendenti sono costituiti principalmente da test delle interfacce esterne, ma comprendono anche test mirati a funzionalità di sicurezza dell'ODV che normalmente non sono raggiungibili dall'esterno:

- modifica delle comunicazioni: implementazione di diverse configurazioni *proxy* al fine di modificare il traffico in tempo reale per verificare il comportamento dell'ODV in situazioni di violazione del protocollo TLS.

Il PP [PP-VIRT] e l'EP [PP-EPSV] richiedono di effettuare test multipli degli algoritmi crittografici. I Valutatori hanno utilizzato lo strumento di convalida crittografica CAVS per verificare le interfacce crittografiche con i vettori di test forniti per la convalida.

Tutti i test eseguiti dai valutatori, inclusi i test CAVS, sono stati completati con successo, ovvero hanno fornito risultati coerenti con i risultati attesi.

11.3 Analisi delle vulnerabilità e test di intrusione

I Valutatori hanno consultato fonti di informazioni di dominio pubblico per identificare vulnerabilità note da verificare mediante esecuzione di test di intrusione. Tale ricerca non ha prodotto risultati.

Per quanto riguarda i test di intrusione derivati dall'analisi indipendente delle vulnerabilità, i Valutatori hanno identificato un totale di due casi di test. Mentre il primo caso di test è stato mirato ad identificare interfacce aggiuntive che avrebbero potuto introdurre potenziali debolezze, il secondo caso di test ha avuto lo scopo di sondare esplicitamente i punti deboli dell'interfaccia del server Telnet. Tutti i test sono stati eseguiti al livello dei sottosistemi del progetto dell'ODV, andando a stimolare il sottosistema TCP/IP dell'ODV.

I Valutatori hanno eseguito una scansione delle porte sullo stesso segmento di rete dell'ODV allo scopo di eliminare eventuali interferenze con altri componenti di rete attivi. La scansione è stata effettuata utilizzando lo strumento *nmap*. Come previsto, lo strumento non ha rilevato altre porte aperte sull'ODV oltre alla porta Telnet, necessaria come da progetto per l'instaurazione di connessioni con l'ODV.

Sono stati eseguiti tentativi di provocare deliberatamente errori di tipo *buffer overflow* durante l'immissione delle credenziali dell'utente. Tale test è stato eseguito sia utilizzando i client standard previsti per l'accesso all'ODV, sia dalla riga di comando. Non è stata eseguita alcuna configurazione specifica relativa ad altri componenti di rete attivi. I test non hanno rivelato debolezze. Le immissioni di dati di input sovradimensionati sono state rifiutate con messaggi di errore, in conformità con i risultati attesi.

L'implementazione del protocollo TLS da parte dell'ODV è stata sollecitata con tecniche di *fuzzing* utilizzando una suite di test disponibile pubblicamente. I test non hanno rilevato errori di implementazione o comportamenti anomali dell'ODV.

I Valutatori hanno quindi concluso che l'ODV, nel suo ambiente operativo, è in grado di resistere ad un attaccante che possiede un potenziale di attacco di livello Basic. Non sono state identificate vulnerabilità sfruttabili o residue.