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. 6/17

(Certification No.)

Prodotto: **DB2 v12 for z/OS**
(Product)

Sviluppato da: **IBM Corp.**
(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 Rita Forsi)

Roma, 12 dicembre 2017

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

DB2 v12 for z/OS

OCSI/CERT/ATS/01/2017/RC

Versione 1.0

12 dicembre 2017

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	12/12/2017

2 Indice

3 Elenco degli acronimi

APAR	Authorized Program Analysis Report
CAF	Call Attachment Facility
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
COTS	Commercial Off-The-Shelf
DAC	Discretionary Access Control
DDM	Distributed Data Management
DL/I	Data Language One
DPCM	Decreto del Presidente del Consiglio dei Ministri
DRDA	Distributed Relational Database Architecture
DSN	Data Source Name
DVD	Digital Versatile Disk
EAL	Evaluation Assurance Level
FD:OCA	Formatted Data Object Content Architecture
FMID	Function Module ID
ID	Identifier
ISPF	Interactivity System Product Facility
IT	Information Technology
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
MAC	Mandatory Access Control
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
(R)DBMS	(Relational) Database Management System
RRS	Resource Recovery Service
RRSAF	Resource Recovery Services Attachment Facility
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SMF	System Management Facility
SQL	Structured Query Language
TLS	Transport Layer Security
TOE	Target Of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSO	Time Sharing Option
VSAM	Virtual Storage Access Method

4 Riferimenti

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

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

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

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

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

[CR-RACF] Certification Report for “RACF for z/OS Version 2 Release 2 from IBM Corporation”, BSI-DSZ-CC-1029-2017, BSI, 25 agosto 2017

[DB2-CCG] DB2 v12 for z/OS Requirements for the Common Criteria, SC27-8863-01, IBM Corporation, 15 giugno 2017

[DB2-INST] DB2 v12 for z/OS Installation and Migration Guide, GC19-8851-00, IBM Corporation, 01 ottobre 2016

[DB2-ADM] DB2 v12 for z/OS Administration Guide, SC27-8844-00, IBM Corporation, 01 ottobre 2016

[DBMSPP] Protection Profile for Database Management Systems (Base Package), Version 2.12, BSI-CC-PP-0088-V2, 23 marzo 2017

[ETR] Final Evaluation Technical Report “DB2 v12 for z/OS”, OCSI-ATS-01-2017_ETR_171016_v2, Version 2, atsec information security GmbH, 16 ottobre 2017

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

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

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

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

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

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

[ST-DB2] DB2 v12 for z/OS Security Target, Version 1.8, IBM Corporation, 10 ottobre 2017

[ST-RACF] Security Target for "IBM RACF for z/OS V2R2", Version 4.13, IBM Corporation, giugno 19, 2017

[ST-ZOS] Security Target for "IBM z/OS Version 2 Release 2", Version 10.9, IBM Corporation, 28 agosto 2014

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 "DB2 v12 for z/OS", sviluppato dalla società International Business Machines Corp. (IBM).

L'ODV è una combinazione dei prodotti IBM DB2 v12 e IBM RACF (Resource Access Control Facility) che operano entrambi come sottosistemi all'interno del sistema operativo mainframe IBM z/OS Version2 Release2 (V2R2). DB2 è un database relazionale che include diverse *utility*. RACF è il componente centralizzato che implementa il controllo di accesso nel sistema operativo z/OS, su cui si basa DB2.

Il componente RACF è già stato valutato e certificato come prodotto a sé stante al livello di garanzia EAL5+ (si veda [ST-RACF] e [CR-RACF]). Pertanto, la valutazione dell'ODV è stata effettuata tenendo in considerazione i risultati della valutazione del componente RACF.

RACF è completamente indipendente da DB2 e le funzionalità di sicurezza che fornisce non sono in alcun modo influenzate dal componente DB2 dell'ODV. Tutti i casi in cui DB2 utilizza funzioni generiche di RACF in modo specifico sono implementati all'interno del componente DB2 e sono quindi interamente coperti dalle attività di valutazione specifiche di DB2. I pochi casi in cui funzionalità di RACF forniscono direttamente funzioni di sicurezza all'ODV sono stati adeguatamente coperti nella valutazione del componente RACF. A causa della non interferenza di DB2 con RACF (garantita dalla separazione degli spazi di indirizzamento in z/OS), tutti i risultati della valutazione di RACF possono essere considerati pienamente validi nell'ambito della valutazione di DB2.

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 [ST-DB2], 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 [ST-DB2] 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 "DB2 v12 for z/OS" 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 [ST-DB2], che specifica i requisiti funzionali e di garanzia e l'ambiente operativo previsto.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	DB2 v12 for z/OS
Traguardo di Sicurezza	DB2 v12 for z/OS Security Target, Version 1.8, IBM Corporation, 10 ottobre 2017
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. 4
Conformità a PP	Protection Profile for Database Management Systems (Base Package), Version 2.12, BSI-CC-PP-0088-V2, 23 marzo 2017
Data di inizio della valutazione	2 maggio 2017
Data di fine della valutazione	16 ottobre 2017

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 [ST-DB2].

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 [ST-DB2].

L'ODV è un prodotto costituito dalla combinazione dei seguenti elementi:

- IBM DB2 v12 per z/OS

- IBM Resource Access Control Facility (RACF) compreso in z/OS Version 2 Release 2.

L'ODV è costituito delle applicazioni software DB2 e RACF in esecuzione su una piattaforma costituita dal sistema operativo z/OS V2R2

DB2 è un RDBMS (Relational Database Management System) COTS (Commercial Off-The-Shelf) che opera come sottosistema del sistema operativo z/OS. Si tratta di un sistema multi-utente in grado di supportare un gran numero di utenti concorrenti.

L'implementazione di DB2 consiste in una collezione di spazi di indirizzamento e una serie di *utility* che operano come sottosistema di z/OS e ne utilizzano le funzionalità di sicurezza.

Gli utenti di DB2 utilizzano istruzioni SQL per definire database e gestire il loro contenuto. Le istruzioni SQL possono essere inviate a DB2 sia mediante svariate *attachment facility*, sia mediante comandi diretti da programmi d'utente. Prima di soddisfare le richieste, DB2 verifica che l'utente possieda i diritti necessari per eseguire le azioni richieste.

DB2 per z/OS fornisce anche sicurezza a livello di riga e a livello di colonna.

DB2 utilizza i servizi centralizzati di controllo di accesso e di gestione della sicurezza forniti dal componente RACF di z/OS per molte delle sue decisioni di accesso. RACF è il componente centralizzato di z/OS responsabile per l'autenticazione degli utenti, il controllo di accesso, la gestione degli attributi di sicurezza degli utenti e la gestione dei diritti di accesso.

I requisiti funzionali di sicurezza (SFR) dell'ODV sono realizzati dalle seguenti funzioni di sicurezza:

- Identificazione e autenticazione
- Controllo di accesso discrezionale
- Audit
- Riutilizzo degli oggetti
- Gestione della sicurezza

Queste funzioni sono descritte con maggiore dettaglio nel capitolo 7.3.2.3.

7.3.1 Architettura dell'ODV

7.3.1.1 Hardware

L'ODV opera come sottosistema del sistema operativo z/OS V2R2. Pertanto, la piattaforma di *runtime* richiesta per l'ODV è la stessa del sistema operativo sottostante.

L'ODV viene eseguito in una partizione logica fornita da una versione certificata di PR/SM su una z/Architecture implementata da una delle seguenti piattaforme hardware:

- IBM zEnterprise 114 con CPACF DES/TDES Enablement Feature 3863 attiva, con almeno una scheda Crypto Express3, con o senza la zEnterprise BladeCenter Extension (zBX).

- IBM zEnterprise 196 con CPACF DES/TDES Enablement Feature 3863 attiva, con almeno una scheda Crypto Express3, con o senza la zEnterprise BladeCenter Extension (zBX).

- IBM zEnterprise zEC12 con CPACF DES/TDES Enablement Feature 3863 attiva, con almeno una scheda Crypto Express3 o Crypto Express4S, con o senza la zEnterprise BladeCenter Extension (zBX).

- IBM z13 con CPACF DES/TDES Enablement Features 3863 attiva, con almeno una scheda Crypto Express4, Crypto Express4S e Crypto Express5S, con o senza la zEnterprise BladeCenter Extension (zBX).

Inoltre, l'ODV può essere eseguito su una macchina virtuale fornita da una versione certificata di z/VM.

Ulteriori dettagli sui requisiti hardware sono contenuti nel capitolo "TOE description" del Traguardo di Sicurezza di z/OS V2R2 [ST-ZOS].

7.3.1.2 Software

L'ODV è costituito da IBM DB2 Versione 12 e IBM RACF per il sistema operativo z/OS Version 2 Release 2, come descritto nel Traguardo di Sicurezza [DB2-ST].

Per una descrizione delle caratteristiche di sicurezza e della configurazione di RACF per z/OS V2R2 si faccia riferimento al capitolo 1.4 "TOE description" del Traguardo di Sicurezza di RACF [ST-RACF]. Nel seguito sono illustrate solamente le funzionalità di DB2.

DB2 è un RDBMS che opera come sottosistema di z/OS. DB2 consiste in una collezione di spazi di indirizzamento e una serie di *utility*.

Gli utenti possono accedere a DB2 localmente mediante le *attachment facility* o da remoto utilizzando la Distributed Data Facility che sfrutta i protocolli DRDA definiti negli Open Group Technical Standard DRDA-V1, DRDA-V2 e DRDA-V3.

Le *attachment facility* vengono eseguite nello spazio di indirizzamento del chiamante e comunicano con lo spazio di indirizzamento di DB2 per espletare le richieste dell'utente. La configurazione valutata dell'ODV include la *attachment facility* TSO che usa il processore di comandi DSN TSO o i pannelli DB2I ISPF (che a loro volta usano DSN per comunicare con DB2).

Un'altra *attachment facility* inclusa nell'ODV è la Call Attachment Facility (CAF) che consente a programmi in esecuzione in ambiente TSO o come *batch* z/OS di comunicare con DB2.

La Resource Recovery Services Attachment Facility (RRSAF) è un'implementazione più moderna di CAF con capacità aggiuntive. RRS è una funzionalità di z/OS che coordina

l'elaborazione di *commit* di risorse recuperabili in un sistema z/OS. DB2 supporta l'uso di questi servizi per applicazioni DB2 che utilizzano la *attachment facility* RRS fornita con DB2. RRS può essere utilizzata per accedere a risorse come tabelle SQL, database DL/I, messaggi MQSeries e file VSAM recuperabili in un singolo ambito di transazione.

Un richiedente che utilizza DRDA si connette ad un server di applicazioni o ad un server di database. DRDA utilizza le architetture Distributed Data Management (DDM) e Formatted Data Object Content Architecture (FD:OCA). DDM è un'architettura di comunicazione che consente lo scambio di messaggi tra sistemi remoti. L'architettura FD:OCA viene utilizzata per scambiare dati d'utente tra sistemi anche eterogenei. Ciò consente ad utenti esterni di connettersi a DB2 e di operare su database DB2.

Le *utility* DB2 sono una serie di programmi accessibili sia online, sia localmente, che forniscono agli amministratori funzioni di diagnostica e di manutenzione dei database. Le *utility* non sfruttano le *attachment facility* standard e operano direttamente sui file dei database a livello di *tablespace*.

La Figura 1 mostra la struttura di base di DB2 e le *attachment facility* supportate nella configurazione valutata.

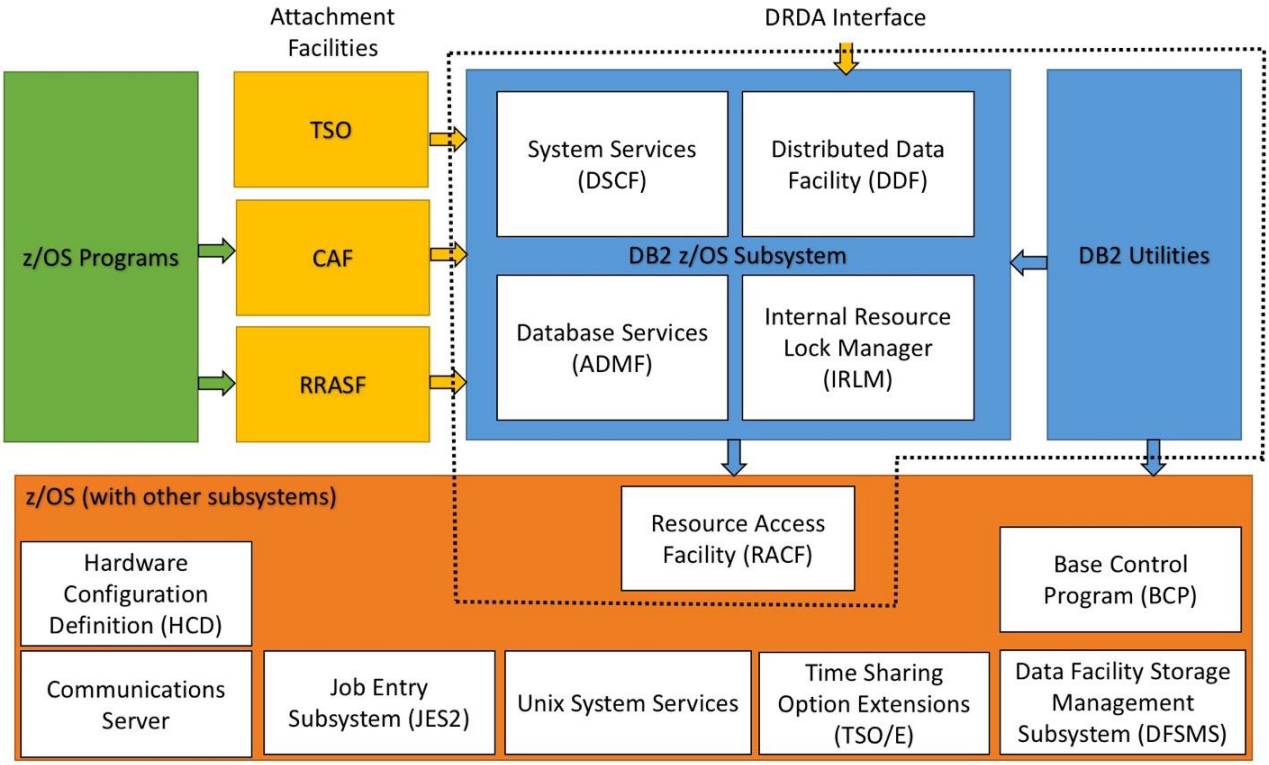

Figura 1 - Struttura di base di DB2 per z/OS

I riquadri blu in figura rappresentano le porzioni attendibili di DB2; i riquadri gialli rappresentano le porzioni delle *attachment facility* di DB2 che vengono eseguite nello spazio di indirizzamento dell'utente o connessioni che utilizzano l'interfaccia di rete. Il riquadro marrone rappresenta il sistema z/OS, ossia la piattaforma dell'ODV che include anche RACF. Il riquadro verde rappresenta programmi utente non attendibili che utilizzano servizi di z/OS e DB2.

Le frecce gialle in figura rappresentano interfacce esterne delle porzioni attendibili di DB2. Le frecce blu rappresentano l'interfaccia tra la porzione attendibile di DB2 e quella di z/OS.

La linea punteggiata delimita il confine dell'ODV.

Si noti che la figura mostra le parti principali dell'ODV e le sue interfacce, non un flusso di informazioni. Va anche sottolineato che le interfacce non sono rappresentate in maniera disgiunta. Ad esempio, le porzioni attendibili di DB2 hanno interfacce con le porzioni attendibili di z/OS che vengono utilizzate anche da altri programmi che girano su z/OS.

Per una descrizione dettagliata dell'ODV, si faccia riferimento al capitolo "TOE description" del Traguardo di Sicurezza [ST-DB2].

7.3.2 Caratteristiche di Sicurezza dell'ODV

7.3.2.1 Politica di sicurezza

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

- **Audit**: sulla base della politica di *audit*, L'ODV registra l'accesso degli utenti e degli amministratori al sistema. L'ampiezza e il dettaglio dell'*audit* sono configurabili.
- **Identificazione e Autenticazione:** tutti gli utenti dell'ODV vengono identificati e autenticati in base al database degli utenti del sistema operativo sottostante. L'autenticazione si basa sui nomi utente, sulle credenziali di autenticazione, sull'appartenenza a gruppi, sulla limitazione delle sessioni concorrenti, sul tempo di accesso al sistema e sulle informazioni di contesto attendibili.
- **Controllo di accesso discrezionale**: l'accesso agli oggetti dell'ODV è protetto richiedendo l'identificazione e l'autenticazione degli utenti e, a valle di questa, controllando l'accesso sulla base di diversi attributi:
    - i privilegi dell'utente per i singoli oggetti dell'ODV;
    - i privilegi di tipo autoritativo dell'utente;
    - i proprietari degli oggetti;
    - i ruoli;
    - i permessi di riga e di colonna.
- **Gestione della sicurezza**: gli amministratori possono gestire:
    - gli attributi di sicurezza degli utenti;
    - i privilegi degli oggetti ed il loro utilizzo da parte degli utenti;
    - i contesti attendibili e i ruoli associati;
    - i permessi di riga e di colonna;

- l'ampiezza dell'audit.

- **Protezione delle informazioni residue**: è impedita la divulgazione di dati ad un altro utente potenziale se lo spazio di memoria precedentemente utilizzato da un oggetto viene riallocato per un altro oggetto.

7.3.2.2 Obiettivi di sicurezza dell'ambiente operativo

Le ipotesi definite nel Traguardo di Sicurezza [ST-DB2] ed alcuni aspetti delle minacce e delle politiche di sicurezza organizzative non sono coperte dall'ODV stesso. Tali aspetti implicano che specifici obiettivi di sicurezza debbano essere soddisfatti dall'ambiente operativo dell'ODV. In particolare, in tale ambito i seguenti aspetti sono da considerare di rilievo:

- I responsabili del sottosistema DB2 sono competenti, fidati e in grado di gestire correttamente il sottosistema e la sicurezza delle informazioni che contiene.

- I responsabili del sottosistema DB2 devono stabilire ed attuare procedure per garantire che le informazioni siano protette in modo appropriato. In particolare, essi devono verificare che:

  - Tutti i cablaggi di rete e delle periferiche siano adeguati per la trasmissione dei dati più sensibili. Si assume che tali collegamenti fisici siano adeguatamente protetti contro le minacce alla riservatezza e all'integrità dei dati trasmessi mediante opportune tecniche di protezione fisica e logica.

  - Le impostazioni di controllo di accesso discrezionale sui file rilevanti per la sicurezza (ad es., tracce di audit e database di autorizzazione) siano configurate correttamente.

  - Gli utenti che hanno necessità di accedere a porzioni di dati gestite dal sottosistema DB2 siano autorizzati e addestrati ad esercitare il controllo sui propri dati.

- Nel sottosistema DB2 non devono essere presenti programmi di calcolo di uso generale, come compilatori o applicazioni d'utente, oltre a quelli necessari per l'operatività, l'amministrazione e il supporto di DB2.

- Tutte le informazioni fornite da entità attendibili nell'ambiente e utilizzate per autenticare e autorizzare l'accesso al sottosistema DB2 debbono essere corrette e aggiornate.

- Nel caso in cui il sottosistema DB2 dipenda dal supporto di sistemi IT esterni attendibili per l'applicazione della politica di sicurezza, tali sistemi devono fornire le funzionalità necessarie a proteggere in modo adeguato l'ambiente da eventuali attacchi che potrebbero compromettere gli obiettivi di sicurezza IT.

- I sistemi IT esterni attendibili devono implementare i protocolli e i meccanismi richiesti dalle funzioni di sicurezza dell'ODV (TSF) per l'applicazione della politica di sicurezza e debbono essere gestiti in base a politiche note, accettate e attendibili, e nel rispetto delle regole applicabili al sottosistema DB2.

- I responsabili del sottosistema DB2 devono garantire che le parti del sottosistema critiche per l'applicazione della politica di sicurezza siano protette da attacchi fisici che potrebbero compromettere gli obiettivi di sicurezza IT. La protezione deve essere commisurata al valore delle risorse IT protette dal sottosistema DB2.

7.3.2.3 Funzioni di sicurezza

Le funzionalità di sicurezza implementate dall'ODV sono descritte in dettaglio nel capitolo 1.4.3 del Traguardo di Sicurezza [ST-DB2]. Di seguito sono riassunti gli aspetti più rilevanti:

- **Identificazione e autenticazione**: la funzionalità di identificazione e autenticazione degli utenti è fornita dal componente RACF. RACF supporta sia password, sia *passphrase* per l'autenticazione. Per le decisioni di accesso relative ai database, DB2 utilizza gli ID di autorizzazione, ossia gli ID utente di RACF più i relativi attributi e ruoli associati all'utente. DB2 utilizza RACF per tutte le decisioni di accesso. La gestione degli utenti e dei loro attributi (inclusi ruoli utente e dati di autenticazione) viene eseguita interamente tramite RACF.

- **Controllo di accesso discrezionale in DB2**: oltre a fornire meccanismi di controllo di accesso, RACF viene utilizzato anche per il controllo di accesso discrezionale agli oggetti DB2. Sono definite classi RACF specifiche che vengono utilizzate per i profili RACF che proteggono le risorse DB2. I profili RACF sono correlati alle autorità degli oggetti DB2 dedicati. Un utente può utilizzare un'autorità specifica per un oggetto DB2 se ha accesso all'autorità in base al proprio ruolo utente (autorità amministrativa DB2) o in base al diritto di accesso che gli è stato assegnato nella lista di accesso del profilo che protegge l'autorità di accesso alla risorsa (privilegi espliciti DB2). A seconda del tipo di oggetto e dell'autorità richiesta, l'utente può utilizzare l'autorità anche quando è proprietario dell'oggetto (privilegi impliciti DB2).
  DB2 consente anche la proprietà di oggetti a partire dai ruoli di database. Un ruolo di database può essere proprietario di oggetti di un database, eliminando la necessità che ogni singolo utente debba possedere e controllare gli oggetti del database; un ruolo di database può essere assegnato ad un singolo utente o ad un gruppo di utenti, offrendo così un meccanismo ulteriore rispetto agli ID di autorizzazione per l'assegnazione di privilegi ed autorizzazioni. I ruoli di database possono essere applicati in un contesto attendibile: un'entità di database basata su un ID di autorizzazione di sistema e un insieme di attributi di attendibilità di connessione.
  DB2 consente inoltre l'applicazione del controllo di accesso sulle tabelle a livello di riga e di colonna attraverso i filtri e le maschere:

    - Un'autorizzazione di riga è un oggetto DB2 collegato a una tabella che specifica, sotto forma di una condizione di ricerca SQL, le condizioni alle quali un utente, un gruppo o un ruolo possono accedere alle righe dei dati nella tabella. È possibile definire più condizioni di riga per una tabella.

    - Analogamente, una maschera di colonna è un oggetto DB2 che specifica, sotto forma di un'espressione SQL di tipo CASE, le condizioni alle quali un utente, un gruppo o un ruolo possono ricevere i valori mascherati restituiti per una colonna. Per ogni colonna può essere definita una sola maschera di colonna.

- **Audit**: In aggiunta alla funzionalità di *audit* fornita dalla piattaforma z/OS, DB2 è in grado di generare record di *audit* nell'ambito del proprio meccanismo di registrazione. Questi record di *audit* vengono memorizzati anche in insiemi di dati SMF. L'*utility* DSN1SMFP fornita in DB2 è in grado di estrarre ed elaborare tali record di audit.
  DB2 consente di configurare la funzionalità di *audit* anche sulla base di politiche di *audit*.

- **Funzionalità di riutilizzo degli oggetti**: DB2 consente il riutilizzo degli oggetti all'interno dei propri spazi di indirizzamento, inclusi gli oggetti del DBMS DB2 controllati dal sottosistema DB2, responsabile dell'implementazione della funzionalità di riutilizzo per questo tipo di oggetti. DB2 utilizza insiemi di dati di z/OS per implementare i propri oggetti e per memorizzare le proprie informazioni di controllo interno.

- **Gestione della sicurezza**: La funzionalità di gestione della sicurezza include sia i ruoli di gestione di DB2, sia i ruoli di gestione definiti da RACF.
  Gli amministratori di DB2 possono eseguire azioni amministrative sui database DB2. DB2 definisce una gerarchia di privilegi che può essere utilizzata per definire un insieme gerarchico di ruoli per la gestione di database DB2.

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 [ST-DB2].

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

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [ST-DB2] dichiara conformità *strict* al seguente Profilo di Protezione (PP):

- [DBMSPP] Protection Profile for Database Management Systems (Base Package), Version 2.12, BSI-CC-PP-0088-V2, 23 marzo 2017.

7.6 Requisiti funzionali e di garanzia

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

Tutti i Requisiti Funzionali di Sicurezza (SFR) sono stati selezionati o derivati per estensione dai CC Parte 2 [CC2]. Il Traguardo di Sicurezza include il seguente componente esteso tratto dal PP [DBMSPP], a cui dichiara conformità *strict*: FIA_USB_(EXT).2 *Enhanced user-subject binding*.

Il Traguardo di Sicurezza [ST-DB2], 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 [ST-DB2], 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 16 ottobre 2017 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [ETR] che è stato approvato dall'Organismo di Certificazione il 30 ottobre 2017. 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 [ST-DB2], 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 "DB2 v12 for z/OS" 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 [ST-DB2] e nella configurazione valutata, riportata in Appendice B – Configurazione valutata.

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia EAL4, con 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 1 – Verdetti finali per i requisiti di garanzia

8.2 Raccomandazioni

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

Si raccomanda ai potenziali acquirenti del prodotto "DB2 v12 for z/OS" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [ST-DB2].

L'ODV deve essere utilizzato in accordo all'ambiente di sicurezza specificato nel capitolo 4.2 del Traguardo di Sicurezza [ST-DB2]. 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 ([DB2-CCG], [DB2-INST], and [DB2-ADM]).

Si assume che l'ODV funzioni in modo sicuro qualora vengano rispettate le ipotesi sull'ambiente operativo descritte nel par. 3.2 del documento [ST-DB2]. 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 fidati sui quali l'ODV si basa per supportare la realizzazione della sua politica di sicurezza. Le specifiche dell'ambiente operativo sono descritte nel documento [ST-DB2].

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

L'ODV viene fornito sotto forma di ServerPac (un insieme preconfigurato di moduli software) memorizzato su una cartuccia o su un DVD che viene fisicamente spedito al cliente. L'ODV viene installato dal cliente mediante le finestre di dialogo di installazione di CustomPac. Gli aggiornamenti software (PTF - *Program Temporary Fix*) applicabili all'ODV sono disponibili per il *download* in formato elettronico. Le PTF del componente DB2 e quelle di RACF debbono essere scaricate dal sito Web ShopzSeries di IBM.

La procedura di consegna dell'ODV è composta da una serie di processi che portano alla produzione e alla spedizione dei componenti dell'ODV (ServerPac). La procedura inizia quando la versione finale dell'ODV esce dal processo di sviluppo e viene consegnata all'impianto di produzione, dove i vari componenti vengono caricati sugli appositi supporti, imballati e infine consegnati al cliente.

In Tabella 2 sono elencati i materiali dell'ODV che vengono consegnati al cliente.

#	Tipologia	Identificativo	Release	Metodo di consegna
1	software	RACF	RACF for z/OS V2R2	supporto fisico (nastro)
2	software	DB2 con una delle opzioni di licenza seguenti: • DB2 Version 12 for z/OS (standard version) – product number 5650-DB2 • DB2 Version 12 for z/OS (Value Unit Edition "VUE") - product number 5770-AF3	12	supporto fisico (nastro o DVD)
3	software	DB2 Utilities Suite for z/OS, V12.1 (program number 5770-AF4)	12	supporto fisico (nastro o DVD)
4	aggiornamenti software (PTF)	DB2: • UI48030 (APAR PI69090) • UI48033 (APAR PI79654) • UI41325 (APAR PI69172) • UI45206 (APAR PI74886) RACF: • OA48557 • OA49499 • OA49703 • PI53376 • PI53852 • PI54933 • OA48941 • OA49458 • OA49992 • OA50235 • OA50314 • OA50306 • OA50969 • OA51185	-	download sicuro (via ShopzSeries)

#	Tipologia	Identificativo	Release	Metodo di consegna
5	documentazione	DB2: • DB2 v12 for z/OS Common Criteria Guide (SC27-8863) • DB2 v12 for z/OS What's New? (GC27-8861) • DB2 v12 for z/OS Introduction to DB2 for z/OS (SC27-8852) • DB2 v12 for z/OS Installation and Migration Guide (GC18-8851) • DB2 v12 for z/OS Administration Guide (SC27-8844) • DB2 v12 for z/OS Command Reference (SC27-8848) • DB2 v12 for z/OS Managing Security Guide (SC27-8854) • DB2 v12 for z/OS RACF Access Control Module Guide (SC27-8858) • DB2 v12 for z/OS Data Sharing: Planning and Administration (SC27-8849) • DB2 v12 for z/OS Codes (GC27-8847) • DB2 v12 for z/OS Messages (GC27-8855) • DB2 v12 for z/OS Application Programming Guide and Reference for Java™ (SC19 SC27-8846) • DB2 v12 for z/OS Application Programming and SQL Guide (SC27-8845) • DB2 v12 for z/OS SQL Reference (SC27-8859) • DB2 v12 for z/OS Utility Guide and Reference (SC27-8860) RACF: • z/OS V2R2 Planning for Multilevel Security and the Common Criteria (GA32-0891-01) • z/OS V2R2 - Security Server RACF Auditor's Guide (SA23-2290-01) • z/OS V2R2 - Security Server RACF Command Language Reference (SA23-2292-01) • z/OS V2R2 - Security Server RACF Callable Services (SA23-2293-01) • z/OS V2R2 - Security Server RACF Data Areas (GA32-0885-01) • z/OS V2R2 - Security Server RACF Diagnosis Guide (GA32-0886-01) • z/OS V2R2 - Security Server RACF Macros and Interfaces (SA23-2288-01) • z/OS V2R2 - Security Server RACF Messages and Codes (SA23-2291-01) • z/OS V2R2 - Security Server RACROUTE Macro Reference (SA23-2294-01) • z/OS V2R2 - Security Server RACF Security Administrator's Guide (SA23-2289-01) • z/OS V2R2 - Security Server RACF System Programmer's Guide (SA23-2287-01) • z/OS V2R2 - Security Server RACF General User's Guide (SA23-2298-01)	12	documentazione DB2: supporto fisico (DVD) documentazione RACF: download sicuro

Tabella 2 - Materiali consegnabili dell'ODV

9.2 Identificazione dell'ODV

L'ODV può essere identificato dal cliente nei seguenti due modi:

- verificando il nome univoco e la versione del prodotto, ossia "DB2 v12 for z/OS" (come indicato nel TDS, sulla pagina di *download* del produttore e sulla documentazione di guida);
- mediante i numeri di prodotto (numeri univoci a sette cifre) e i codici FMID (*Function Module ID*) dei componenti installabili del prodotto consegnati su supporto fisico e delle PTF aggiuntive scaricabili.

9.3 Installazione, inizializzazione ed utilizzo sicuro dell'ODV

L'installazione dell'ODV comprende due parti: 1) il pacchetto base valutato CC fornito su supporto fisico e 2) le PTF scaricate, o "service delivery", applicate al pacchetto base.

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

In particolare, i seguenti documenti contengono informazioni per l'inizializzazione sicura dell'ODV e la preparazione del suo ambiente operativo in conformità con gli obiettivi di sicurezza specificati nel Traguardo di Sicurezza [ST-DB2]:

- DB2 v12 for z/OS Requirements for the Common Criteria [DB2-CCG];
- DB2 v12 for z/OS Installation and Migration Guide [DB2-INST];
- DB2 v12 for z/OS Administration Guide [DB2-ADM].

10 Appendice B – Configurazione valutata

L'installazione dell'ODV comprende i seguenti elementi software:

- Il pacchetto DB2 v12 composto da:
  - una delle due versioni seguenti di DB2 v12 for z/OS:
    - DB2 v12 for z/OS edizione standard (product number 5650-DB2)
    - DB2 v12 for z/OS VUE (*Value Unit Edition*) (product number 5770-AF3).
  - DB2 Utilities Suite for z/OS v12.1 (program number 5770-AF4)
- Il componente di controllo d'accesso RACF for z/OS V2R2, come specificato nel relativo Traguardo di Sicurezza [ST-RACF].

Tutti gli APAR forniti con i due pacchetti devono essere installati come descritto nei memo forniti con i pacchetti stessi.

Le due versioni di DB2 v12 per z/OS sono praticamente identiche: la differenza tra le due opzioni di spedizione si riferisce alla licenza del prodotto, non alla sua funzionalità.

Inoltre, entrambe le versioni di DB2 v12 per z/OS includono diversi FMID che implementano funzionalità escluse dalla configurazione valutata. Questi componenti sono disabilitati durante l'installazione dell'ODV e pertanto sono esclusi dall'ambito dell'ODV:

- HIYCC10 IMS Attach
- JDBCC12 JDB12/SQLJ
- JDBCC17 ODBC

Il componente RACF Remote Sharing Facility (RRSF) non è stato incluso nella valutazione e pertanto non deve essere utilizzato nella configurazione valutata dell'ODV.

Per maggiori dettagli sulla configurazione valutata si faccia rifermento al documento [DB2-CCG].

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+ 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 Fornitore ha predisposto una piattaforma di test completamente automatizzata comprendente 160 casi di test, suddivisi in diversi file per ogni caso di test secondario, in cui ogni file consente di verificare diverse funzionalità e parametri delle interfacce. Questa piattaforma è stata utilizzata per verificare tutte le funzioni di sicurezza dichiarate nel TDS e tutte le interfacce relative ai diversi sottosistemi, nei contesti DAC e MAC. Sono stati conservati file di mappatura separati per le interfacce/sottosistemi e le funzioni di sicurezza.

Il Fornitore ha inoltre registrato la data dell'esecuzione corretta di ciascun caso di test in una tabella riassuntiva. L'ambiente di test è stato realizzato mediante diversi sistemi virtualizzati di DB2 su z/OS che hanno consentito di verificare le funzionalità ad accesso remoto. La maggior parte dell'attività di test si è concentrata sulla verifica della corretta applicazione dei privilegi di accesso, che costituisce la parte prevalente delle TSF. In generale, l'approccio ai test ha consentito di effettuare verifiche molto approfondite e di dettaglio.

La descrizione dei casi di test è incorporata nei file di test e contiene riferimenti espliciti alle finalità di ciascun test.

L'ambiente di test è stato potenziato da *script* che verificano che i diversi server di test siano ancora attivi durante lo svolgimento delle prove. Ulteriori *script* hanno permesso di invertire l'ordine di esecuzione dei casi di test allo scopo di dimostrare che non esistono interdipendenze.

Il sistema di test fornito è un ambiente virtualizzato su z/VM. L'uso di diverse macchine virtuali ha consentito l'effettuazione di test distribuiti. Le sessioni di test sono state condotte utilizzando lo strumento di test TCPUN installato su tutte le macchine. Ogni sistema compreso nell'ambiente di test è stato configurato staticamente con le opzioni di RACF richieste da z/OS e quelle specifiche per la versione valutata CC di DB2, inclusa la definizione degli utenti in RACF. Mediante gli *script* di test, sono state impostate dinamicamente le opzioni necessarie a consentire i contesti DAC e MAC, mentre i privilegi e le autorizzazioni degli utenti sono stati impostati dinamicamente secondo necessità da ogni singolo caso di test. L'ambiente di test è stato reso disponibile da remoto. I file di test sono stati memorizzati su un sistema z/VM.

La configurazione dell'ODV è stata effettuata seguendo quanto riportato nel TDS e nella documentazione per la configurazione valutata, con alcune eccezioni che non hanno

influito sulla validità dei risultati dei test (ad es., non sono state rispettate le indicazioni per la robustezza delle password e sono state utilizzate connessioni non TLS).

I valutatori hanno utilizzato la piattaforma di test messa a disposizione dal Fornitore per eseguire sia i test funzionali indipendenti, sia quelli di intrusione.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Approccio adottato per i test

L'approccio del Fornitore è stato quello di dimostrare che i test effettuati consentono di verificare il corretto funzionamento di tutte le funzioni di sicurezza dichiarate nel TDS e di tutte le interfacce relative ai diversi sottosistemi.

11.2.2 Copertura dei test

Le funzionalità dell'ODV sono state coperte dai test fino al livello dei sottosistemi e i Valutatori hanno potuto verificare che i percorsi di esecuzione più rilevanti sono stati presi in considerazione. La maggior parte dei casi di test fa riferimento direttamente a specifici capitoli della documentazione di guida, con citazione di alcuni paragrafi, onde semplificare la preparazione e l'esecuzione dei test riguardanti comportamenti specifici dell'ODV. Ogni comportamento testato è stato verificato utilizzando, ove possibile, diversi livelli di privilegi; ad es., sono state impiegate utenze amministrative, utenze con privilegi espliciti per una specifica attività o utenze non privilegiate, per la verifica dei casi negativi.

11.2.3 Risultati dei test

La ripetizione dei test proposti dal Fornitore ha dato esito positivo nella totalità dei casi.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

11.3.1 Approccio adottato per i test

I Valutatori hanno ripetuto 2 delle 3 serie di test funzionali rilevanti per l'ODV sviluppati dal Fornitore. I Valutatori hanno inoltre predisposto 11 test indipendenti utilizzando come base i test del Fornitore.

I Valutatori hanno rieseguito i test del Fornitore nella cosiddetta modalità ad accesso controllato. I test del Fornitore relativi alle etichette di sicurezza non sono stati eseguiti in quanto non rilevanti per la valutazione, dato che questa funzionalità non è inclusa nel TDS. I file relativi ai casi di test del Fornitore sono stati memorizzati su un sistema z/VM connesso con le macchine di test. I valutatori hanno utilizzato questi sistemi per l'accesso e l'esecuzione di ogni caso di test, sia singolarmente, sia in gruppi.

I Valutatori hanno utilizzato lo strumento di test TCPUN per eseguire i casi di test e per verificare un eventuale esito negativo di uno qualsiasi dei test. Questo strumento di test produce un file di risultato per ogni caso di test fallito e diversi file di riepilogo dei risultati per tutti i test appartenenti ad una serie specifica di test. In alcuni casi, i Valutatori hanno utilizzato le opzioni dello strumento di test anche per generare i file di output per i casi di test, inclusi quelli con esito positivo. Questo è stato fatto allo scopo di verificare la logica di

confronto dello strumento utilizzata per comparare i risultati reali dei test con quelli attesi contenuti nei file di verifica predisposti.

Tutti i test indipendenti sono stati eseguiti nell'ambiente di test messo a disposizione dal Fornitore. I test indipendenti sono stati ideati per coprire casi in cui il Fornitore non ha testato tutte le autorità amministrative o per verificare combinazioni aggiuntive di impostazioni dei permessi per nuove funzioni.

11.3.2 Copertura dei test

La riesecuzione dei test del Fornitore ha permesso di coprire la maggior parte delle interfacce e dei relativi sottosistemi. I test indipendenti predisposti dai Valutatori hanno ampliato la copertura allo scopo di verificare diverse combinazioni di autorità amministrative e privilegi per nuove funzioni, aumentando il rigore del test, già molto approfonditi, delle funzionalità di controllo di accesso.

11.3.3 Risultati dei test

Tutti i test sono stati eseguiti con successo e non è stata rilevata alcuna deviazione dai risultati attesi.

11.4 Analisi delle vulnerabilità e test di intrusione

11.4.1 Approccio adottato per i test

I Valutatori hanno preso in considerazione fonti pubbliche per le vulnerabilità note di DB2 e hanno selezionato solamente quelle che risultano applicabili alla versione z/OS del prodotto. I Valutatori hanno predisposto test relativamente ai seguenti aspetti:

- esecuzione di eventi di trigger successivamente alla modifica dei privilegi dell'utente che ha creato il trigger (interfaccia SQL per la *attachment facility* TSO locale);
- test con input DRDA malformato o derivante da *fuzzing*, focalizzati su descrittori e dati FDO:CA (interfaccia DRDA);
- verifica della presenza di *account* predefiniti (interfaccia DRDA);

I test del protocollo DRDA sono stati realizzati utilizzando codice Java/Groovy che ricrea in parte un proprio client DRDA per poter inserire i valori di input malformati laddove necessario.

I test si sono concentrati sulla modalità di accesso remoto all'ODV mediante l'interfaccia DRDA; ciò ha consentito ai Valutatori di eseguire test più approfonditi su specifici aspetti di DRDA, in particolare sulla parte del protocollo relativa alla specifica dei dati FDO:CA. Si è preferito utilizzare questo approccio mirato, invece di un approccio in cui un certo numero di funzionalità non sarebbero state verificate in maniera così approfondita, in quanto il Fornitore ha già eseguito una serie completa di casi di test che coprono tutti gli aspetti delle TSF. Inoltre, eventuali vulnerabilità sfruttabili da remoto risulterebbero in genere molto più critiche per l'ODV.

L'obiettivo è stato quello di rivelare qualsiasi comportamento anomalo dell'ODV che a sua volta potrebbe essere indice di potenziali falle più gravi potenzialmente sfruttabili, come ad esempio condizioni di *buffer overflow* o altri difetti a livello di codice. In aggiunta ai test sul protocollo DRDA, i Valutatori hanno verificato il corretto utilizzo dei *trigger* nel caso in cui i privilegi assegnati all'utente al momento della creazione del *trigger* risultano rimossi all'istante di attivazione dell'evento reale di *trigger*. Un altro test ha riguardato la verifica della presenza di un ID d'utente predefinito di cui si è trovato riferimento nella documentazione di guida.

11.4.2 Copertura dei test

Obiettivo principale è stato quello di eseguire test approfonditi sul protocollo DRDA (sostituendo i singoli valori dei parametri del protocollo con dati non validi o di lunghezza errata e inviando grandi blocchi di dati nel flusso delle *query*). Tutti i test hanno utilizzato le interfacce dell'ODV accessibili dall'esterno e sono stati stimolati i sottosistemi Distributed Data Services Subsystem (nella maggior parte dei test DRDA), Relational Data Subsystem e System Services Subsystem.

11.4.3 Risultati dei test

Tutti i test sono stati eseguiti con successo. I risultati delle prove di intrusione non hanno rilevato la presenza di vulnerabilità dell'ODV sfruttabili nell'ambiente operativo dichiarato.