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)*

This page is intentionally left blank

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

DB2 v12 for z/OS

OCSI/CERT/ATS/01/2017/RC

Version 1.0

12 December 2017

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	12/12/2017

2 Table of contents

3 Acronyms

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
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 References

[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

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

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

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

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

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

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

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

5 Recognition of the certificate

5.1 International Recognition of CC Certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA]) has been ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on http://www.commoncriteriaportal.org.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA up to EAL2.

6 Statement of Certification

The Target of Evaluation (TOE) is the product “DB2 v12 for z/OS”, developed by International Business Machines Corp. (IBM).

The TOE is a combination of IBM DB2 v12 and IBM RACF (Resource Access Control Facility), which both operate as subsystems within IBM z/OS, Version 2 Release 2 (V2R2) mainframe operating system. DB2 is a relational database including database utilities. RACF is the central access control component of the z/OS operating system leveraged by DB2.

The RACF component has previously been evaluated and certified at EAL5+ as a separate product (see [ST-RACF], and [CR-RACF]). Therefore, the TOE evaluation has been conducted keeping into account the results of the RACF component evaluation.

RACF is completely independent from DB2, so any security functionality it provides is not influenced by the DB2 component of the TOE. All cases where DB2 uses generic RACF functions in a specific way are implemented within the DB2 component and therefore fully covered by the DB2-specific evaluation activities. The few cases where RACF functionality directly provides TOE security functionality have been appropriately covered in the evaluation of the RACF component. Because of the non interference of DB2 with RACF (enforced by the address space separation in z/OS), all the RACF evaluation results remain fully valid for the DB2 evaluation.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST-DB2]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL4, augmented with ALC_FLR.3, according to the information provided in the Security Target [ST-DB2] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product “DB2 v12 for z/OS” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [ST-DB2], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	DB2 v12 for z/OS
Security Target	DB2 v12 for z/OS Security Target, Version 1.8, IBM Corporation, 10 October 2017
Evaluation Assurance Level	EAL4 augmented with ALC_FLR.3
Developer	IBM Corporation
Sponsor	IBM Corporation
LVS	atsec information security GmbH
CC version	3.1 Rev. 4
PP conformance claim	Protection Profile for Database Management Systems (Base Package), Version 2.12, BSI-CC-PP-0088-V2, 23 March 2017
Evaluation starting date	2 May 2017
Evaluation ending date	16 October 2017

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST-DB2] are met.

7.3 Evaluated product

This section summarizes the main functional and security features of the TOE; for a detailed description, please refer to the Security Target [ST-DB2].

The TOE is a combined product, consisting of the following elements:

- IBM DB2 v12 for z/OS
- IBM Resource Access Control Facility (RACF) as part of z/OS Version 2 Release 2.

The TOE are the DB2 and RACF software applications running on a z/OS V2R2 operating system platform.

DB2 is a COTS (Commercial Off-The-Shelf) RDBMS (Relational Database Management System) that operates as a subsystem of the z/OS operating system. It is a multi-user system with the ability to support many concurrent users.

DB2 is implemented by a set of address spaces plus a set of utilities operating as a subsystem of z/OS and uses the security functionality of z/OS.

DB2 users can use SQL statements to define databases and manage their content. Several “attachment facilities” exist that can be used to submit SQL statements as well as database commands from user programs to DB2. DB2 will evaluate the user’s right to perform the requested actions before satisfying the request.

DB2 for z/OS also provides row-level and column-level security.

DB2 uses the central access control and security management services provided by the Resource Access Control Facility (RACF) of z/OS for many of its access decisions. RACF is the central component within z/OS responsible for user authentication, access control, management of user security attributes, and management of access rights.

TOE’s security functional requirements (SFRs) are realized by the following security functions:

- Identification & authentication
- Discretionary access control
- Audit
- Object re-use
- Security management

These functions are described more in detail in sect. 7.3.2.3.

7.3.1 TOE Architecture

7.3.1.1 Hardware

The TOE operates as a subsystem within the z/OS V2R2 operating system. Therefore, the required runtime platform for the TOE is the same as the operating system.

The TOE is running within a logical partition provided by a certified version of PR/SM, on the z/Architecture as implemented by the following hardware platforms:

- IBM zEnterprise 114 with CPACF DES/TDES Enablement Feature 3863 active, with at least one Crypto Express3 card, and with or without the zEnterprise BladeCenter Extension (zBX).

- IBM zEnterprise 196 with CPACF DES/TDES Enablement Feature 3863 active, with at least one Crypto Express3 card, and with or without the zEnterprise BladeCenter Extension (zBX).

- IBM zEnterprise zEC12 with CPACF DES/TDES Enablement Feature 3863 active, with at least one Crypto Express3 or Crypto Express4S card, and with or without the zEnterprise BladeCenter Extension (zBX).

- IBM z13 with CPACF DES/TDES Enablement Features 3863 active, with at least one Crypto Express4, Crypto Express4S and Crypto Express5S cards, with or without the zEnterprise BladeCenter Extension (zBX).

In addition, the TOE may run on a virtual machine provided by a certified version of z/VM.

Please refer to the “TOE description” section of z/OS V2R2 Security Target [ST-ZOS] for further details on hardware requirements.

7.3.1.2 Software

The TOE is the IBM DB2 Version 12 for z/OS with IBM RACF for z/OS Version 2 Release 2 operating system as described in the Security Target [DB2-ST].

The security description and configuration of the RACF for z/OS V2R2 is provided in section 1.4 “TOE description” of the RACF Security Target [ST-RACF]. Only the DB2-specific functionality is described below.

DB2 is a RDBMS that operates as a subsystem of z/OS. DB2 is implemented by a set of address spaces plus a set of utilities.

Users can access DB2 locally using “attachment facilities” or remotely via the Distributed Data Facility which uses the DRDA protocols defined in the Open Group Technical Standards DRDA-V1, DRDA-V2, and DRDA-V3.

Attachment facilities execute in the caller’s address space and communicate with the DB2 address spaces to serve requests from the user. Attachment facilities included in the evaluated configuration include the TSO attachment facility via the DSN TSO command or the DB2I ISPF panels (which in turn use the DSN command to communicate with DB2).

Another attachment facility is the Call Attachment Facility (CAF), which allows programs executing under TSO or in the z/OS batch environment to communicate with DB2.

The Resource Recovery Services Attachment Facility (RRSAF) is a newer implementation of CAF with additional capabilities. RRS is a feature of z/OS that coordinates commit processing of recoverable resources in a z/OS system. DB2 supports use of these services for DB2 applications that use the RRS attachment facility provided with DB2. Use the RRS attachment to access resources such as SQL tables, DL/I databases, MQSeries messages, and recoverable VSAM files within a single transaction scope.

A requester using DRDA connects to an application server or database server. DRDA uses Distributed Data Management (DDM) and Formatted Data Object Content Architecture (FD:OCA) as part of the underlying architecture of DRDA. DDM is the

communication language used for message interchange systems. FD:OCA is used to exchange user data among like or unlike systems. This allows external users to connect to DB2 and operate on DB2 databases.

The DB2 Utilities are a set of online and standalone programs providing database diagnostic and maintenance functions for administrators. The utilities do not use the standard attachment facilities and operate with the database files directly at the tablespace level.

Figure 1 shows the basic structure of DB2 and the attachment facilities supported in the evaluated configuration.

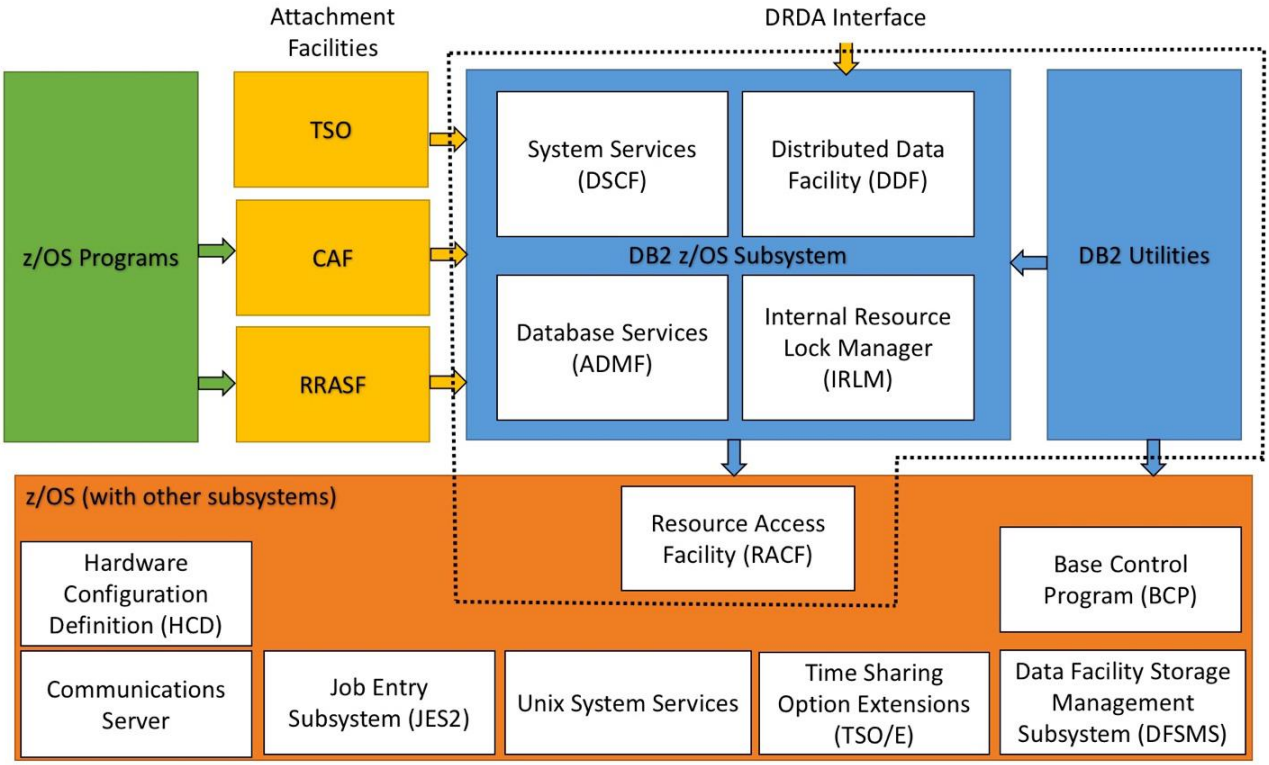

Figure 1 - Basic structure of DB2 for z/OS showing TOE structure with TOE boundary

The blue boxes in this figure represent the trusted parts of DB2, the yellow boxes represent those parts of the attachment facilities of DB2 executing in the user's address space or connections using the network interface. The brown box represents the z/OS system as the platform of this TOE, which also includes RACF. The green box represents (untrusted) user programs using services of z/OS and DB2.

The yellow arrows in the figure represent external interfaces of the trusted parts of DB2. The blue arrows represent the interface between the trusted part of DB2 and the trusted part of z/OS.

The dotted line shows the boundary of the TOE.

It should be noted that this figure shows the main parts of the TOE and its interfaces, not a flow of information. It should also be noted that the interfaces are not disjointed. The

trusted parts of DB2, for example, will also use interfaces to the trusted parts of z/OS that are also used by other programs operating on top of z/OS.

For a detailed description of the TOE, please refer to the “TOE description” section of the Security Target [ST-DB2].

7.3.2 TOE security features

7.3.2.1 Security policy

The security policy enforced is defined by the selected set of Security Functional Requirements and implemented by the TOE. It covers the following policies:

- **Auditing**: Based on the Audit Policy, the TOE monitors access of users and administrators to the system. The extent and detail of the auditing is configurable.
- **Identification & Authentication:** All users of the TOE are identified and authenticated, based on the user database of the underlying operating system. The authentication considers user names, authentication credentials, groups membership, limitation of concurrent sessions, time of system access, and trusted context information.
- **Discretionary access control**: Access to TOE objects is protected by requiring identification and authentication of users, and based on that, by controlling access through various means:
    - user privileges for individual TOE objects;
    - user authoritative privileges;
    - object ownership;
    - roles;
    - row and column permissions.
- **Security management**: Administrators can manage:
    - user security attributes;
    - objects privileges and their use by users;
    - trusted contexts and associated roles;
    - row and column permissions;
    - the extent of auditing.
- **Residual information protection**: Prevent disclosure of data to a potential other user if previous object memory space gets reallocated for another object.

7.3.2.2 Operational environment security objectives

The Assumptions defined in the Security Target [ST-DB2] and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE operational environment. The following topics are of relevance:

- Individuals responsible for the DB2 subsystem are competent, trustworthy, and capable of managing the subsystem and the security of the information it contains.
- Individuals responsible for the DB2 subsystem must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular, they must complete the following tasks:
    - All network and peripheral cabling must be approved for the transmittal of the most sensitive data. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques.
    - Discretionary access control protections on security-relevant files (such as audit trails and authorization databases) must be set up correctly.
    - Users must be authorized if they need to access parts of the data managed by the DB2 subsystem and trained to exercise control over their own data.
- There are no general-purpose computing capabilities, such as compilers or user applications, available on the DB2 subsystem, other than those services necessary for DB2 operation, administration, and support.
- Any information provided by a trusted entity in the environment and used for authorizing and authenticating access to the DB2 subsystem is correct and up to date.
- If the DB2 subsystem relies on remote trusted IT systems to support the enforcement of the security policy, those systems must provide the required functions to sufficiently protect the environment from any attack that might compromise IT security objectives.
- The remote trusted IT systems must implement the protocols and mechanisms required by the TOE security functions (TSF) to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted, and trusted policies as well as the rules applicable to the DB2 subsystem.
- Individuals responsible for the DB2 subsystem must ensure that the parts of the subsystem critical to the enforcement of the security policy are protected from physical attacks that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the DB2 subsystem.

7.3.2.3 Security functions

The TOE security functionality is described in detail in sect. 1.4.3 of the Security Target [ST-DB2]. The most significant aspects are summarized below:

- **Identification & authentication**: The RACF component provides user identification and authentication. RACF supports passwords and passphrases for user authentication. DB2 uses authorization IDs, which is the RACF user ID together with its associated attributes and user roles, for access decisions to and within databases. DB2 uses RACF to make such access decisions. All management of users and their attributes (including user roles and authentication data) is performed through RACF.

- **Discretionary access control in DB2**: In addition to the access control mechanisms provided by the RACF component, RACF is also used for the discretionary access control to DB2 objects. Specific RACF classes are defined that are used for RACF profiles protecting DB2 resources. The RACF profiles are related to authorities of dedicated DB2 objects. A user can use a specific authority for a DB2 object, if he either has access to the authority based on his user role (DB2 administrative authority), or has access based on the access right he has been assigned in the access list of the profile protecting the authority to the resource (DB2 explicit privilege). Depending on the type of object and the authority requested, he may also use the authority when he is the owner of the object (DB2 implicit privilege).
  DB2 also allows object ownership by database roles. A database role can own database objects, which helps eliminate the need for individual users to own and control database objects; instead, the database role is then assigned to an individual user or a group of users, thus offering a mechanism other than authorization IDs through which privileges and authorities can be assigned. Database roles are applicable in a trusted context: a database entity based on a system authorization ID and a set of connection trust attributes.
  DB2 also allows the enforcement of access control on tables at row and column levels through filtering and data masking:

  - A row permission is a DB2 object linked to a table that specifies in the form of an SQL search condition the conditions under which a user, group or role can access the rows of data in the table. Multiple row conditions can be defined for a table.

  - Similarly, a column mask is a DB2 object that specifies, in the form of an SQL case expression, the conditions under which a user, group or role can received the masked values that are returned for a column. Only one column mask can be defined for a column.

- **Audit**: In addition to the audit functionality provided by the z/OS platform, DB2 is able to generate audit records as part of the DB2 trace mechanism. Those audit records are also stored in the SMF data sets. The DSN1SMFP utility provided in DB2 is able to extract and process those audit records.
  DB2 also allows the configuration of the audit functionality based on audit policies.

- **Object re-use functionality**: Within the DB2 address spaces, DB2 itself provides object reuse including DB2 DBMS objects that are controlled by the DB2 subsystem, which is responsible to implement object reuse for those objects. DB2 uses z/OS data sets to implement the DB2 objects and to store DB2 internal control information.

- **Security management**: Security Management functionality includes both the DB2 management roles and the RACF defined management roles.
  DB2 administrators are allowed to perform administrative actions for DB2 databases. DB2 defines a hierarchy of privileges that can be used to define a hierarchical set of roles for the administration of DB2 databases.

7.4 Documentation

The guidance documentation specified in Annex A - Guidelines for secure usage of the TOE is delivered to the customer together with the product. The guidance documentation contains all the information for installation, configuration and secure usage of the TOE in accordance with the requirements of the Security Target [ST-DB2].

Customers should also follow the recommendations for the secure usage of the TOE contained in sect. 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST-DB2] claims strict conformance to the following Protection Profile:

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

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

All Security Functional Requirements (SFR) have been selected or derived by extension from CC Part 2 [CC2]. In particular, considering that the Security Target claims strict conformance to the [DBMSPP] PP, the following extended component from such PP is included: FIA_USB_(EXT).2 Enhanced user-subject binding.

Please refer to the Security Target [ST-DB2] for a complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST-DB2]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body (OCSI) has supervised the conduct of the evaluation performed by the evaluation facility (LVS) atsec information security GmbH.

The evaluation was completed on 16 October 2017 with the issuance by LVS of the Evaluation Technical Report [ETR], which was approved by the Certification Body on 30 October 2017. Then, the Certification Body issued this Certification Report.

7.8 General considerations on the validity of the certification

The evaluation focused on the security features declared in the Security Target [ST-DB2], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; it remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR] issued by the LVS atsec information security GmbH and documents required for the certification, and considering the evaluation activities carried out, the Certification Body (OCSI) concluded that TOE "DB2 v12 for z/OS" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4, augmented with ALC_FLR.3, with respect to the security features described in the Security Target [ST-DB2] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL4, augmented with ALC_FLR.3.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Basic modular design	ADV_TDS.3	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass
Delivery procedures	ALC_DEL.1	Pass

Assurance classes and components		Verdict
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
Well-defined development tools	ALC_TAT.1	Pass
Systematic flaw remediation	*ALC_FLR.3*	Pass
Tests	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Focused vulnerability analysis	AVA_VAN.3	Pass

Table 1 - Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in Section 6 (Statement of Certification).

Potential customers of the product “DB2 v12 for z/OS” are suggested to properly understand the specific purpose of the certification reading this Certification Report together with the Security Target [ST-DB2].

The TOE must be used according to the Security Objectives for the operational environment specified in par. 4.2 of the Security Target [ST-DB2]. Potential customers are advised to check that they meet the identified requirements and to pay attention to the recommendations contained in this Report.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, Annex A - Guidelines for secure usage of the TOE includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([DB2-CCG], [DB2-INST], and [DB2-ADM]).

It is assumed that the TOE can be operated in a secure manner only if the assumptions for the operational environment described in sect. 3.2 of the Security Target [ST-DB2] are respected. In particular, it is assumed that TOE administrators are adequately trained in the correct use of the TOE and selected among the trusted staff of the organization. The TOE is not designed to counter threats from inexperienced, malicious or negligent administrators.

It should also be noted that TOE security is conditioned by the proper functioning of the hardware platforms on which the TOE is installed, and of all trusted external IT systems

supporting the implementation of TOE's security policy. Specifications for the operational environment are described in the Security Target [ST-DB2].

9 Annex A - Guidelines for secure usage of the TOE

This Annex provides considerations particularly relevant to the potential customers of the TOE.

9.1 TOE delivery

The TOE is delivered as a ServerPac (a preconfigured set of software modules) on a cartridge or DVD that is physically shipped to the customer and installed by the customer via CustomPac install dialogs, as well as applicable Program Temporary Fixes (PTFs) that are available for electronic download. These PTFs that are part of DB2 must be obtained using the ShopzSeries IBM website. The RACF PTFs are obtained in the same way.

The delivery of the TOE is a chain of processes to produce and ship the TOE components (ServerPacs). The process starts when the TOE has been built by the developers and delivered to the production facility, where they are collected, packaged, and finally delivered to the customer.

Table 2 lists TOE materials that are delivered to the customer.

#	Type	Identifier	Release	Form of delivery
1	software	RACF	RACF for z/OS V2R2	physical shipment (tape)
2	software	DB2 with one of the following licensing options: • 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	physical shipment (tape or DVD)
3	software	DB2 Utilities Suite for z/OS, V12.1 (program number 5770-AF4)	12	physical shipment (tape or DVD)
4	software updates (PTFs)	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	-	secure download (via ShopzSeries)
5	docs	DB2: • DB2 v12 for z/OS Common Criteria Guide (SC27-	12	DB2 docs: physical shipment

#	Type	Identifier	Release	Form of delivery
		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)		(DVD) RACF docs: secure download

Table 2 - TOE deliverables

9.2 Identification of the TOE

There are two ways of identifying the TOE, as follows:

- the unique name and version such as “DB2 v12 for z/OS” (as listed in the ST, the developer’s download page, and the guidance documentation);

- the product numbers (that is, the unique seven-digit number) and FMIDs (Function Module IDs) of the installable components shipped in each product, as well as additional PTFs not shipped together with the TOE.

9.3 Installation, initialization and secure usage of the TOE

TOE installation consists of two parts: 1) the CC-evaluated base package shipped on physical media and 2) downloaded PTFs, or service deliveries, that are applied to the base package.

TOE installation and configuration should be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the following documents contain information for the secure initialization of the TOE and the preparation of its operational environment in accordance with the security objectives specified in the Security Target [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 Annex B – Evaluated configuration

The TOE requires the following software elements to be installed:

- The DB2 v12 Package:
  - One of the two versions of DB2 v12 for z/OS:
    - the standard DB2 v12 for z/OS (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)
- The RACF for z/OS V2R2 access control component, as specified in the Security Target for IBM RACF for z/OS V2R2 [ST-RACF].

Any APARs delivered with the two packages must be installed as described in the memos delivered with the packages.

Both versions of DB2 v12 for z/OS are almost identical: the difference between the two shipping options relates to the product licensing, not to product functionality.

Additionally, both versions of DB2 v12 for z/OS include several FMIDs that implement functionality excluded in the evaluated configuration. These components are disabled during the TOE installation and therefore they are excluded from the TOE scope:

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

The RACF Remote Sharing Facility (RRSF) is not considered as a part of this evaluation and therefore must not be used in an evaluated system configuration.

The details of the evaluated configuration are documented in [DB2-CCG].

11 Annex C –Test activities

This Annex describes the effort of both Developer and LVS in testing activities. For the assurance level EAL4, augmented with ALC_FLR.3, such activities include the following three steps:

- evaluation of the tests performed by the Developer in terms of coverage and level of detail;
- execution of independent functional tests by the Evaluators;
- execution of penetration tests by the Evaluators.

11.1 Test configuration

The Developer used a fully-automated test suite comprised of 160 test cases, which split up into several sub test case files, where each test case file may test several functions and interface parameters. This test framework was used to test every ST claim, all interface functions, and subsystems, in both DAC and MAC context. Separate mapping files (for interfaces/subsystems and claims) where maintained.

In addition, the Developer used a summary sheet, where the date of the successful execution of each test case was recorded. The test environment was comprised of several virtualized systems of DB2 on z/OS to test remote functionality. Most of the tests focused on testing access privileges, which comprises the biggest portion of the TSF. In general, the testing effort allowed for very focused and fine-grained testing.

The test case description is embedded within the test files and refers explicitly to the test claims.

The test environment was enhanced by scripts that check that the different test servers are still active during testing. Additional test scripts reverse the order of test cases to demonstrate that no interdependencies exist.

The provided test system is a virtualized environment on z/VM. Several VMs allow for distributed testing. The test tool TCPUN is installed on these machines to drive the test suites. The test systems are statically configured with necessary RACF options from z/OS and the DB2 Common Criteria specific settings. This includes defining users in RACF. As part of the test scripts, options are set dynamically to allow for DAC and MAC contexts, and user privileges and authorities are set dynamically as needed by each test case. The test environment was made available remotely. Test files were stored on a z/VM system.

The configuration was made following the ST and guidance for the evaluated configuration with a few exceptions (e.g., password strength guidelines not applied, and non-TLS connections), which did not affect applicability of the test results to the TOE.

Evaluators used the test system provided by the Developer to perform both independent and penetration testing.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer's approach was to demonstrate that all ST claims, interfaces, and subsystems are verified by the tests.

11.2.2 Test coverage

The tested behavior was covered down to the level of subsystems, and the Evaluators could verify that most relevant execution paths were taken into account. Most test cases directly referred to the sections in the guidance and some cited paragraphs to smooth test development and verification with respect to specific TOE behavior. Each tested behavior was tested with different privileges if applicable, e.g., administrative users, users with explicit privileges for the task, or users without privileges (to test the negative case).

11.2.3 Test results

The results of the Developer showed a 100% successful test run.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Testing approach

The Evaluators executed 2 of the 3 relevant Developer test suites. The Evaluators further devised 11 tests using the Developer tests as basis.

The Evaluators executed the Developer test suites in so-called Controlled Access mode. The label security tests of the Developer were not relevant for the evaluation, as this functionality was not claimed in the ST. The Developer test cases were stored on a z/VM that was connected to the test machines. The Evaluators used these systems to access and execute any test case, either individually or as a group.

The Evaluators used the test tool TCPUN to execute the test cases and to determine whether any of the tests failed. The test tool produced a result file for each unsuccessful test case, and summary files on the results for all tests that are part of a test suite. The Evaluators also used options of the tool to generate, in some cases, output files for test cases, even the ones that were successful. This was used to verify the comparison logic of the tool that takes place when comparing the actual results with the provided verification file.

All independent tests were executed on the test environment provided by the Developer. The independent tests were devised to cover cases where the Developer did not test all administrative authorities, or to test additional combinations of permission settings for new functions.

11.3.2 Test coverage

Execution of the Developer tests covered most interfaces and subsystems. The additional Evaluators tests increased the coverage for testing different combinations of administrative

authorities and privileges for new functions (increasing the rigor of the already thorough testing of access control functions).

11.3.3 Test results

The tests were executed successfully, not resulting in any deviation from the expected results.

11.4 Vulnerability analysis and penetration tests

11.4.1 Testing approach

The Evaluators considered common sources for vulnerabilities of DB2 in general and narrowed the findings down to what is applicable to the z/OS version of the product. The Evaluators devised tests related to the following aspects:

- trigger event execution after the privileges of the user who created the trigger changed (SQL interface for local TSO attachment);
- DRDA fuzzing and malformed input tests focused on the FDO:CA descriptors and data (DRDA interface);
- test for default accounts (DRDA interface);

The DRDA protocol tests were defined using Java/Groovy code which partly recreate an own DRDA client to be able to insert the necessary malformed input values where needed.

The tests focused on using remote access to the TOE (using the DRDA interface), which enabled the Evaluators to perform more in-depth tests on specific DRDA aspects, mainly the FDO:CA data specification part of the DRDA protocol specification. This focused approach was favored against an approach where a variety of functionality is not so deeply tested, because the Developer already runs a very thorough suite of test cases on all aspects of the TSF. Also, any remote vulnerabilities are usually much more critical to the TOE.

The goal was to reveal any unstable TOE behavior which in turn indicates potential bigger problems that could be exploited in form of buffer overflows or other software flaws. In addition to the DRDA tests, the Evaluators tested the proper enforcement of trigger situations where user privileges that existed at the time the trigger was created, did not exist at actual trigger event time. Another test was for a default/predefined user ID that was found in the guidance.

11.4.2 Test coverage

The main goal was to perform in-depth tests on the DRDA protocol (exchanging individual protocol parameter values with invalid input, incorrect length parameter, sending large chunks of data for the data query flow). All tests used the externally accessible interfaces of the TOE, and the exercised subsystems were the Distributed Data Services Subsystem (applies to most of the DRDA tests), the Relational Data Subsystem, and the System Services Subsystem.

11.4.3 Test results

The tests were executed successfully. None of the test results indicated any vulnerability of the TOE.