DB2 v12 for z/OS Security Target

Version 1.8

Status: Release

Last Update: 2017-10-10

This document is provided AS IS with no express or implied warranties. Use the information in this document at your own risk.

Document History

Version	Date	Summary	Author
1.8	2017-10-10	Public Version	Clemens Wittinger

Table of Content

1 Introduction 9
1.1 ST reference 9
1.2 TOE reference 9
1.3 TOE overview 9
1.3.1 About The TOE 9
1.3.2 About the non-TOE Software Platform 10
1.4 TOE description 10
1.4.1 Structure of TOE 10
1.4.1.1 RACF 11
1.4.1.2 DB2 12
1.4.1.3 DB2 system structures 13
1.4.2 TOE boundary and interfaces 14
1.4.3 Software security function summary 14
1.4.3.1 Identification and authentication 14
1.4.3.2 Discretionary access control in DB2 15
1.4.3.3 Audit 15
1.4.3.4 Object re-use functionality 15
1.4.3.5 Security management 15
1.4.4 Configurations 15
1.4.4.1 Software configurations 15
1.4.4.2 TOE guidance 17
2 Conformance claims 19
3 Security problem definition 20
3.1 Introduction 20
3.2 Assumptions 20
3.3 Threats 20
3.4 Organizational security policies 21
4 Security objectives 22
4.1 Security objectives for the TOE 22
4.2 Operational environment security objectives 22
4.3 Rationale for the security objectives 23
5 Extended components definition 24
6 Security requirements 25
6.1 TOE security functional requirements 25
6.1.1 Security audit (FAU) 27

6.1.1.1 FAU_GEN.1 Audit data generation 27
6.1.1.2 FAU_GEN.2 User identity association 30
6.1.1.3 FAU_SEL.1 Selective audit 30
6.1.2 User data protection (FDP) 30
6.1.2.1 FDP_ACC.1 Subset access control 30
6.1.2.2 FDP_ACF.1 Security attribute based access control 31
6.1.2.3 FDP_RIP.1 Subset residual information protection 34
6.1.3 Identification and authentication (FIA) 34
6.1.3.1 FIA_ATD.1 User attribute definition 34
6.1.3.2 FIA_UAU.1 Timing of authentication 35
6.1.3.3 FIA_UID.1 User identification before any action 35
6.1.3.4 FIA_USB_(EXT).2 Enhanced user-subject binding 35
6.1.4 Security management (FMT) 36
6.1.4.1 FMT_MOF.1 Management of security functions behavior 36
6.1.4.2 FMT_MSA.1 Management of security attributes 36
6.1.4.3 FMT_MSA.3 Static attribute initialization 36
6.1.4.4 FMT_MTD.1 Management of TSF data 37
6.1.4.5 FMT_REV.1(1) Revocation (Users) 37
6.1.4.6 FMT_REV.1(2) Revocation (Objects) 37
6.1.4.7 FMT_SMF.1 Specification of Management Functions 37
6.1.4.8 FMT_SMR.1 Security roles 38
6.1.5 Protection of the TSF (FPT) 39
6.1.5.1 FPT_TRC.1 Internal TSF consistency 39
6.1.6 TOE Access (FTA) 39
6.1.6.1 FTA_MCS.1 Basic limitation on multiple concurrent sessions 39
6.1.6.2 FTA_TSE.1 TOE session establishment 39
6.2 Security Functional Requirements Rationale 39
6.2.1 Coverage 39
6.2.2 Sufficiency 40
6.2.3 Security Requirements Dependency Analysis 43
6.3 TOE security assurance requirements 43
6.4 Security Assurance Requirements Rationale 43
6.5 TOE Summary Specifications Rationale 43
6.5.1 Security functions justification 43
7 TOE summary specification 45
7.1 Overview of the TOE 45
7.1.1 DB2 Structure and Architecture 46

7.1.2 RACF Structure and Architecture 46
7.2 Identification and authentication 47
7.2.1 Authentication function 47
7.2.2 Special handling in DB2 48
7.2.3 Trusted contexts 48
7.2.4 Session Limits 48
7.3 Access control 49
7.3.1 Access control principles 49
7.3.1.1 The authorization hierarchy 49
7.3.2 RACF-protected resources of DB2 50
7.3.3 Discretionary access control in DB2 51
7.3.3.1 DB2 objects 51
7.3.3.2 DB2 object ownership 53
7.3.4 Access evaluation algorithm for DB2 objects 54
7.3.4.1 DB2 administrative authorities 56
7.3.4.2 DB2 objects for owner ACEE authorization 57
7.3.4.3 Buffer pool privileges 58
7.3.4.4 Collection privileges 58
7.3.4.5 Database privileges 59
7.3.4.6 Java archive privileges 60
7.3.4.7 Package privileges 60
7.3.4.8 Plan privileges 61
7.3.4.9 Role privileges 61
7.3.4.10 Schema privileges 62
7.3.4.11 Sequence privileges 62
7.3.4.12 Storage group privileges 62
7.3.4.13 Stored procedure privileges 62
7.3.4.14 DB2 system privileges 63
7.3.4.15 Table privileges 64
7.3.4.16 Tablespace privileges 66
7.3.4.17 Trusted context privileges 66
7.3.4.18 View privileges 66
7.3.4.19 Global variable privileges 67
7.3.4.20 Trigger Privileges 67
7.3.5 Row and Column access control 68
7.3.5.1 Row permissions 68
7.3.5.2 Column masks 69

7.3.6 DB2 internal access checking 69
7.4 Security management 69
7.4.1 Security management in RACF 69
7.4.1.1 User and Group Management 69
7.4.1.2 Resource Management 71
7.4.1.3 RACF configuration and management 73
7.4.2 Security management of DB2 74
7.4.3 DB2 user attributes and user roles and database roles 75
7.4.4 Trusted contexts and database roles 75
7.4.5 Transfer of Database Object Ownership 76
7.5 Auditing 76
7.5.1 Generation of audit records 76
7.5.2 Event Notifications generated by RACF 77
7.5.3 Audit configuration and management 77
7.5.4 Auditing in DB2 77
7.6 Object reuse 80
7.6.1 Object reuse in DB2 80
8 Abbreviations, Terminology and References 82
8.1 Abbreviations 82
8.2 Terminology 83
8.3 References 85

Table of Figures

Figure 1: Basic structure of DB2 for z/OS showing TOE structure with TOE boundary 11
Figure 2: (Simplified) structure of a DB2 database 13

Table of Tables

Table 1 – Security Functional Requirements for the TOE 26
Table 2 – TOE auditable events 29
Table 3 – Mapping between SFRs and Security Objectives 40
Table 4 – Security objectives for the TOE rationale 43
Table 5 – Mapping of security functional requirements to security functions 44
Table 6 – Object name qualifiers in RACF profiles 53
Table 7 – DB2 administrative authorities...57
Table 8 – Authorization IDs for dynamic SQL 58
Table 9 – Database object privileges 59
Table 10 – Access to specific privileges for databases 60
Table 11 – Package privileges 61
Table 12 – Plan privileges 61
Table 13 – Role privileges..61
Table 14 – Schema privileges 62
Table 15 – Sequence privileges 62
Table 16 – Storage group privileges 62
Table 17 – Stored procedure privileges 63
Table 18 – DB2 system privileges 64
Table 19 - Table privileges 65
Table 20 – Tablespace privileges..66
Table 21 – Trusted context privileges 66
Table 22 – View privileges 67
Table 23 – Global variable privileges 67
Table 24 – Trigger Privileges 68
Table 25 – User Profile...70
Table 26 – Resource Profile Structure 73
Table 27 – Audit classes 79
Table 28 – Audit categories..80

1 Introduction

1.1 ST reference

Title:	DB2 v12 for z/OS Security Target
Version:	1.7.2
Status:	Draft
Date:	2017-05-17
Sponsor:	IBM Corporation ®
Developer:	IBM Corporation
Keywords:	IBM; DB2 v12; DB2 for z/OS; relational database management system (RDBMS); database management system (DBMS); DBMSPP; RACF; access control

1.2 TOE reference

The Target of Evaluation (TOE) is the IBM DB2 v12 for z/OS Version 2 Release 2 including IBM RACF for z/OS Version 2 Release 2.

1.3 TOE overview

The Target of Evaluation (TOE) consists of:

- The “IBM DB2 v12 for z/OS” (DB2 12).
- The IBM Resource Access Control Facility (RACF) as part of z/OS Version 2 Release 2.
- Guidance documentation as described in section 1.4.4.2

1.3.1 About The TOE

The TOE is the DB2 and RACF software application layered on an underlying system (running z/OS V2.2).

DB2 is a commercial-off-the-shelf (COTS) relational database management system (RDBMS) that operates as a subsystem of the operating system, z/OS. 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.

Users can use SQL statements to define databases and manage their content. Several “attach 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.

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

RACF provides the interfaces and implementation for identification and authentication of users using different authentication mechanisms such as passwords or pass-phrases, interfaces that resource managers can use for both discretionary and mandatory access control to objects they define, interfaces for sophisticated security management functions, and the ability to generate audit records for security critical events.

RACF is used in discretionary access control decisions within and by the TOE. DB2 further supports access control by specifying database roles in a trusted context which provides the flexibility for managing context-specific privileges and simplifies the processing of authorization. Additionally, DB2 implements security controls down to the granularity of individual rows in a database.

Access rights for DB2 objects are managed using the interface provided by RACF. Access controls defined by the SQL GRANT and REVOKE commands are ignored in the evaluated version of the TOE since access control to the DB2 objects is provided by RACF.

The TOE provides accountability through the generation of audit records. The TOE also allows to configure the level and scope of the audit functionality.

The TOE comes with management functions that allow configuring the TSF and tailor them to the customer’s needs.

1.3.2 About the non-TOE Software Platform

The non-TOE software platform consists of one instance of z/OS V2.2 running on an abstract machine as the sole operating system exercising full control over it.

The “IBM z/OS Version 2 Release 2” operating system was evaluated under certificate ID BSI-DSZ-CC-0948. The ST for z/OS V2.2 [ZOSST] provides further information about the security functionality provided to DB2 by the platform.

The required runtime environment for the z/OS V2.2 platform is described in section “TOE description” of the z/OS Security Target [ZOSST]. This description is also valid for this TOE and is not restricted or expanded by it.

Multiple instances of the TOE platform may be connected as an enclave, in a basic sysplex or in a parallel sysplex, sharing their RACF database and acting like a single system also in regards to the security functions described in this security target. This functionality is provided by z/OS V2.2 (see [ZOSST]), DB2 and RACF rely on the mechanisms provided by the underlying operating system.

1.4 TOE description

The Target of Evaluation (TOE) is the IBM DB2 v12 for z/OS (DB2) including the IBM Resource Access Control Facility (RACF) for the z/OS Version 2 Release 2 (z/OS V2.2) operating system.

The security description and configuration of the z/OS V2.2 component is provided in the z/OS Security Target [ZOSST] section 1.4 “TOE description”, in this ST only the TOE specific functionality is described.

1.4.1 Structure of TOE

The following figure shows the basic structure of the TOE and DB2 attachment facilities supported in the evaluated configuration.

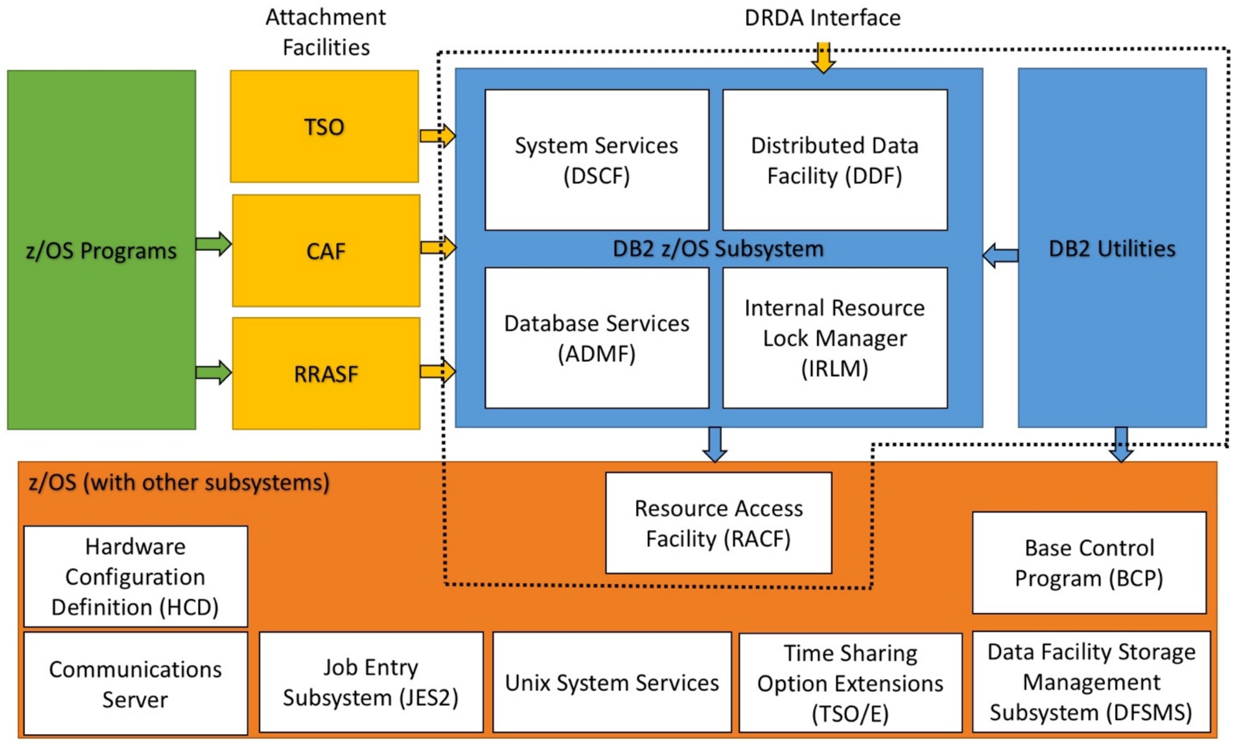
Attachment Facilities
DRDA Interface
z/OS Programs
TSO
CAF
RRASF
System Services (DSCF)
Distributed Data Facility (DDF)
DB2 z/OS Subsystem
Database Services (ADMF)
Internal Resource Lock Manager (IRLM)
DB2 Utilities
z/OS (with other subsystems)
Resource Access Facility (RACF)
Hardware Configuration Definition (HCD)
Base Control Program (BCP)
Communications Server
Job Entry Subsystem (JES2)
Unix System Services
Time Sharing Option Extensions (TSO/E)
Data Facility Storage Management Subsystem (DFSMS)

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 (see section 1.4.1.2), 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 (see section 1.4.1.1). 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 brown arrow represents the external interfaces of the trusted parts of z/OS (which have been assessed in the z/OS evaluation). The blue arrows represent the interface between the trusted part of DB2 and the trusted part of z/OS. The green arrows represent (untrusted) user program interfaces to the attachment facilities of DB2.

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 disjoint. 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.

1.4.1.1 RACF

RACF is the component that is called within z/OS from any component that wants to perform user authentication, access control to protected resources and the management of user security attributes and access rights.

RACF is designed as an authentication and access manager component that manages both user security attributes and access management attributes in its own database. Users are represented within RACF by user profiles and protected resources are represented by resource profiles. Users can be members of groups where each group is represented by a group profile.

Resource profiles are structured into classes, which represent the different types of resources. Within such a class a individual profile is represented by the name of the resource, which is unique within its class. Resource manager will then query RACF whenever they need to check a user's access rights to a resource. In this query they will specify the resource class, the name of the resource within the class, the type of access requested and the internal representation of the user that requests access.

RACF is also called when a component within z/OS needs to authenticate a user. In this case the z/OS component will call RACF and will pass the identity of the user, the authentication credentials presented, the name of the component requesting user authentication and several other parameters to RACF. Based on this information RACF will authenticate the user and, if successful, create a control block representing the user with the security attributes assigned. This control block is later used when a component of z/OS calls RACF for checking access rights.

RACF also provides interfaces that allow the management of user profiles, digital certificates assigned to users, group profiles, resource profiles, access rights and general RACF attributes. RACF also provides an interface that z/OS components can call to generate a security related audit record.

1.4.1.2 DB2

DB2 is a relational database management system that operates as a subsystem of z/OS. DB2 is implemented by a set of z/OS 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.

1.4.1.2.1 DB2 objects

DB2 implements the following DB2 objects in the following object hierarchy:

- Subsystem or data sharing group
  - Database
    - Table space
      - Table
        - Column
        - Row
    - Index space
      - Index
  - View

In addition to those, DB2 implements the following other objects:

- Storage group
- Buffer pool

- Plan
- Role (known as database role in this ST)
- Collection
  - Package
- Schema
  - Stored procedure
  - user-defined function – not in evaluated configuration
  - Java ARchive (JAR) – not in evaluated configuration
  - User-defined type – not in evaluated configuration
  - Sequence
  - Row permission
  - Column mask
- Trusted context
- Global variable
- Trigger

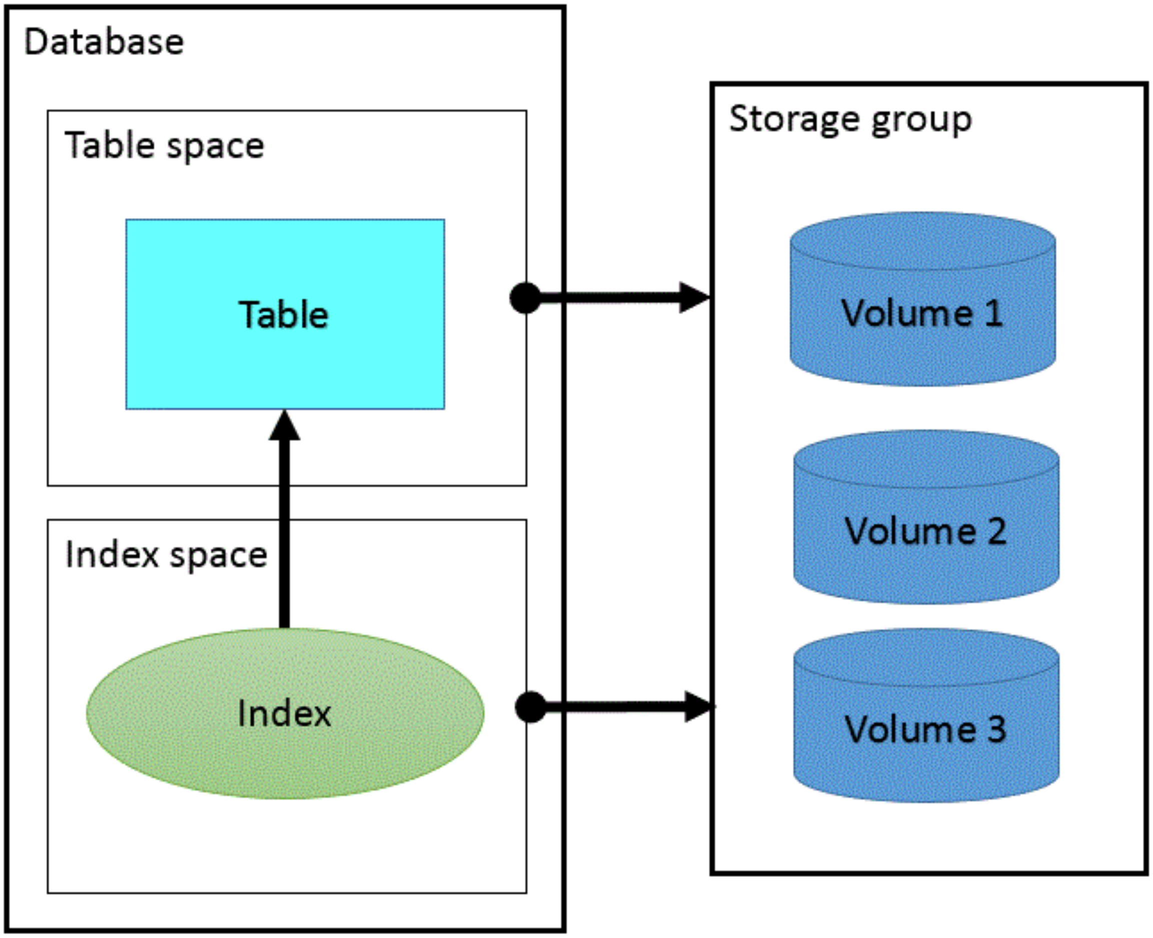

Figure 2: (Simplified) structure of a DB2 database

1.4.1.3 DB2 system structures

DB2 has a comprehensive infrastructure that enables it to provide data integrity, performance, and the ability to recover user data. Unlike the DB2 data structures that users create and access, DB2 controls and accesses system structures. The system structures that this section describes are:

- Catalog
- Active and archive logs

- Bootstrap data set

1.4.1.3.1 Catalog

DB2 maintains a set of tables that contain information about the data that is under its control. These tables are collectively known as the catalog. The catalog tables contain information about DB2 objects such as tables, views, and indexes. When you create, alter, or drop an object, DB2 inserts, updates, or deletes rows of the catalog that describe the object.

1.4.1.3.2 Active and archive logs

DB2 is able to record all data changes and other significant events in a log. By having this record of changes, DB2 can re-create those changes in the event of a failure. DB2 can even roll the changes back to a previous point in time.

DB2 writes each log record to a disk data set called the active log. When the active log is full, DB2 copies the contents of the active log to a disk or magnetic tape data set called the archive log.

The logging attributes, LOGGED or NOT LOGGED can be specified at table space level. The ability to suspend record logging is useful in situations in which data is being duplicated and loss of concurrency and recoverability is not a concern. In those cases, if the data is lost, it can be re-created or regenerated from the original source instead of using an image copy and applying log records.

Note: data logging and the audit facility are different features in DB2.

1.4.1.3.3 Bootstrap data set

The bootstrap data set (BSDS) contains information that is critical to DB2, such as the names of the logs. DB2 uses information in the BSDS for system restarts and for any activity that requires reading the log.

1.4.2 TOE boundary and interfaces

The trusted part of the TOE consists of all TOE code operating in supervisor state, operating with a storage key of 0 to 7 or operating with APF authorization. This includes the code operating in the DB2 address spaces as well as the RACF code operating with the above mentioned privileges. Since RACF provides the identification and authentication as well as parts of the access control functionality for DB2, this component is part of the TOE.

RACF has been evaluated previously at the EAL5+ level and relevant results of this evaluation are taken into account as part of this evaluation. The basic security requirements and security functions of RACF are defined in the RACF Security Target document [RACFST].

1.4.3 Software security function summary

The TOE provides the security functionality listed below and explained in the following subsections:

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

These primary security features are supported by domain separation and reference mediation, which ensure that the features are always invoked and cannot be bypassed.

1.4.3.1 Identification and authentication

The RACF component provides user identification and authentication. RACF supports passwords and pass-phrase in user authentication.The RACF user ID and its associated attributes and user roles are used by DB2 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.

1.4.3.2 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.

1.4.3.3 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.

1.4.3.4 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.

1.4.3.5 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.

1.4.4 Configurations

1.4.4.1 Software configurations

The Target of Evaluation requires the following software elements to be installed:

- The Common Criteria Evaluated Base for DB2 V12 Package, which includes:
  - One of the two versions of DB2 v12 for z/OS:
    - the standard DB2 v12 for z/OS (program number 5650-DB2)

        - DB2 v12 for z/OS VUE (value unit edition) (program number 5770-AF3), which delivers a one-time-charge price metric for Eligible Workloads.
    - DB2 Utilities Suite for z/OS, V12.1 (program number 5770-AF4)
- The Common Criteria IBM RACF for z/OS V2R2 access control component (certificate ID BSI-DSZ-CC-1029), as specified in the Security Target for IBM RACF for z/OS V2R2 ([RACFST]).

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 only difference between the standard version and the VUE version is that the latter includes an additional FMID. FMID JDB991Z VUE License agreement (5770-AF3) adds SMP/e jobs and special ISPF panels for the DB2 installation CLIST which allow administrators to indicate whether a particular DB2 is to operate under the terms of the DB2 v12 for z/OS VUE license.

In case the licensing option is chosen, DB2 v12 for z/OS VUE requires running in a logical partition (LPAR) on z/OS V2.2 configured as zNALC (System z New Application License Charges).

Additionally, both versions of DB2 v12 for z/OS include several FMIDs that implements 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.

NOTE: There are no claims for cryptographic functions in this ST. Hence, certificate-based user authentication is out of scope.

1.4.4.1.1 DB2 installation options and restrictions

The following options and elements must be installed in the evaluated configuration:

- Audit traces
- Install SYSADM and Install SYSOPR roles for the initial setup and configuration of DB2. (Note that you must disable the Install SYSADM and Install SYSOPR roles after installation).
- RACF authorization exit (DSNXRXAC)
- Subsystem security
- TCP/IP, if you use distributed data

You can use the following options and elements without changing the security characteristics of the evaluated configuration:

- Call attachment facility
- TSO attachment facility
- RRSAF attachment facility
- DB2 utilities

The following objects, options, and elements must not be configured for use, or must be deactivated:

- Administrative stored procedures
- Administrative task scheduler
- CICS® connections
- Data propagation products
- Encryption and decryption built-in functions
- GRANT/REVOKE functions

- IMS Attach (FMID: HIYCC10)
- Java Archives (JAR)
- JDBC/SQLJ (FMID: JDBCC12)
- Kerberos
- ODBC/CLI (FMID: JDBCC17)
- PassTickets
- Secondary authorization IDs
- Sign-on authorization IDs
- SNA™ connections
- Unified debugger
- z/OS ODBC interface to SQL
- DB2 Web Services
- MQSeries user-defined functions
- User exit routines
- z/OSMF Installation
- REST API

In the DB2 configuration package the following must be set –

- routine, and statement caching must be turned off
- “EXTENDED SECURITY” must be set to “NO”
- “AUTH EXIT CHECK” must be set to “DB2”

– following the guidance provided in the “DB2 12 Requirements for the Common Criteria Guide” [SC27-8863].

To operate the TOE, the evaluated version of the product must be installed in their evaluated version and configured in a secure manner as described in the directions delivered with the installation media and especially for DB2: “DB2 12 Requirements for the Common Criteria Guide” [SC27-8863] and “DB2 v12 for z/OS Administration Guide" [SC27-8844].

1.4.4.2 TOE guidance

The following documents are part of the product documentation and are relevant for the secure operation of the TOE:

- 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)

- 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)

2 Conformance claims

This Security Target is [CC] *Part 2 extended* and *Part 3 conformant*, with a claimed Evaluation Assurance Level of EAL 4, augmented by ALC_FLR.3. The Common Criteria version 3.1 revision 4 has been taken as the basis for this conformance claim.

This Security Target makes a claim of strict conformance on the following Protection Profile.

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

This Protection Profile has been evaluated and is listed on the BSI web site as a validated protection profile (certification ID BSI-CC-PP-0088-V2). See [BSI-PP] for more information.

3 Security problem definition

3.1 Introduction

The statement of the TOE security problem definition describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be deployed.

To this end, the statement of the TOE security environment identifies the list of assumptions made on the operational environment (including physical and procedural measures) and the intended method of use of the product, defines the threats that the product is designed to counter, and the organizational security policies with which the product is designed to comply.

This Security Target claims conformance to the Base Protection Profile for Database Management Systems [DDMSPP]. The Assumptions, Threats and Organizational Security Policies, together with extensions defined in the Protection Profile are taken over without change from the protection profile.

3.2 Assumptions

This Security Target includes all assumptions defined in section 4.5 “Assumptions” of the Protection Profile [DBMSPP]. There are no additional assumptions defined in this Security Target.

A.PHYSICAL: It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

A.AUTHUSER: Authorized users possess the necessary authorization to access at least some of the information managed by the TOE.

A.MANAGE: The TOE security functionality is managed by one or more competent individuals. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.

A.TRAINEDUSER: Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.

A.NO_GENERAL_PURPOSE: There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration, and support of the DBMS.

A.PEER_FUNC_&_MGT: All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.

A.SUPPORT: Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is used by the TOE is correct and up to date.

A.CONNECT: All connections to and from remote trusted IT systems and between separate parts of the TSF are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.

3.3 Threats

This Security Target includes all threats defined in section 4.3 “Threats” of the Protection Profile [DBMSPP]. There are no additional threats defined in this Security Target.

T.ACCESS.TSFDATA: A threat agent may read or modify TSF data using functions of the TOE without the proper authorization.

T.ACCESS.TSFFUNC: A threat agent may use or manage TSF, bypassing the protection mechanisms of the TSF.

T.IA.MASQUERADE: A user or a process acting on behalf of a user may masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources.

T.IA.USER: A threat agent may gain access to user data, TSF data, or TOE resources with the exception of public objects without being identified and authenticated.

T.RESIDUAL_DATA: A user or a process acting on behalf of a user may gain unauthorized access to user or TSF data through reallocation of TOE resources from one user or process to another.

T.TSF_COMPROMISE: A user or a process acting on behalf of a user may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable code within the TSF.

T.UNAUTHORIZED_ACCESS: A threat agent may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.

3.4 Organizational security policies

This Security Target includes all organizational security policies defined in section 4.4 “Organizational Security Policies” of the Protection Profile [DBMSPP]. There are no additional organizational security policies defined in this Security Target.

P.ACCOUNTABILITY: The authorized users of the TOE shall be held accountable for their actions within the TOE.

P.ROLES: Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible supporting only the administrative duties the person has. This role shall be separate and distinct from other authorized users.

P.USER: Authority shall only be given to users who are trusted to perform the actions correctly.

4 Security objectives

This section defines the security objectives of the TSF and its supporting environment. Security objectives, categorized as either IT security objectives or non-IT security objectives, reflect the stated intent to counter identified threats, comply with any organizational security policies identified, or both. All of the identified threats and organizational policies are addressed under one of the following categories.

4.1 Security objectives for the TOE

This Security Target includes all security objectives defined in section 5 “Security Objectives” of the Protection Profile [DBMSPP]. There are no additional security objectives defined in this Security Target.

O.ADMIN_ROLE: The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.

O.AUDIT_GENERATION: The TSF must be able to record defined security-relevant events (which usually include security-critical actions of users of the TOE). The information recorded for security-relevant events must contain the time and date the event happened and, if possible, the identification of the user that caused the event, and must be in sufficient detail to help the authorized user detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.

O.DISCRETIONARY.ACCESS: The TSF must control access of subjects and/or users to named resources based on identity of the object. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.

O.I&A: The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.

O.MANAGE: The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality..

O.MEDIATE: The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.

O.RESIDUAL_INFORMATION: The TOE will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.

O.TOE_ACCESS: The TOE will provide functionality that controls a user's logical access to user data and to the TSF.

4.2 Operational environment security objectives

This Security Target includes all operational environment security objectives defined in section 5.2 “Operation Environment Security Objectives” of the Protection Profile [DBMSPP]. There are no additional operational environment security objectives defined in this Security Target.

OE.ADMIN: Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.

OE.INFO_PROTECT: Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular:

> All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. 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.

DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly.

Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.

OE.NO_GENERAL_ PURPOSE: There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration, and support of the DBMS.

OE.PHYSICAL: Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.

OE.IT_I&A: Any information provided by a trusted entity in the environment and used to support user authentication and authorization used by the TOE is correct and up to date.

OE.IT_REMOTE: If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions, required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.

OE.IT_TRUSTED_SYSTEM: The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.

4.3 Rationale for the security objectives

As described in the previous sections of this chapter, the security objectives of the TSF and its supporting environment and the security problem definition of this ST are comprised of those defined in [DBMSPP] and are taken over without change. The rationales for the security objectives and security problem definition provided in that document are also applicable to this ST and therefore not repeated here.

5 Extended components definition

This ST does not define extended components; only the extensions defined in [DBMSPP] are used, they are named here for reference:

[DBMSPP] defines one extended component, which is instantiated in this security target:

- FIA_USB_(EXT).2 Enhanced user-subject binding

6 Security requirements

6.1 TOE security functional requirements

This section defines the functional requirements for the TOE. Functional requirement components in this Security Target were drawn from the Base Protection Profile for Database management ([DBMSPP]), Part 2 of the CC.

CC-defined operations for assignment, selection, and refinement were used to tailor the requirements to the level of detail necessary to meet the stated security objectives. This ST adopts the following convention for operations performed on security functional components:

- Operations already performed in [DBMSPP] and its extensions are kept without any special formatting.
- Refinement operations are marked in **bold** text or in the case of deletions by, ~~**crossed out bold text.**~~
- Selection operations are marked by *italicized text*.
- Assignments operations appear in square brackets with an indication that an assignment has been made [assignment].

Name	Title	D	DB2	RACF	A	S	R	I
FAU_GEN.1	Audit data generation	CC	✓		✓		✓	
FAU_GEN.2	User identity association	CC	✓	✓	✓			
FAU_SEL.1	Selective audit	CC	✓	✓		✓		
FDP_ACC.1	Subset access control	CC	✓	✓				
FDP_ACF.1	Security attribute based access control	CC	✓	✓	✓			
FDP_RIP.1	Subset residual information protection	CC	✓		✓			
FIA_ATD.1	User attribute definition	CC	✓	✓	✓		✓	
FIA_UAU.1	Timing of authentication	CC	✓	✓	✓			
FIA_UID.1	Timing of identification	CC	✓	✓	✓			
FIA_USB_(EXT).2	Enhanced user subject binding	PP	✓	✓	✓			
FMT_MOF.1	Management of security functions behavior	CC	✓	✓	-			
FMT_MSA.1	Management of object security attributes	CC	✓	✓				
FMT_MSA.3	Static attribute initialization	CC	✓	✓				
FMT_MTD.1	Management of TSF data	CC	✓	✓				
FMT_REV.1(1)	Revocation (user attributes)	CC	✓	✓	✓			✓
FMT_REV.1(2)	Revocation (subject, object attributes)	CC	✓	✓	✓			✓
FMT_SMF.1	Specification of Management Functions	CC	✓	✓	✓			
FMT_SMR.1	Security roles	CC	✓	✓	✓		✓	
FPT_TRC.1	Internal TSF consistency	CC	✓		✓			
FTA_MCS.1	Basic limitation on multiple concurrent sessions	CC	✓	✓	✓			

Name	Title	D	DB2	RACF	A	S	R	I
FTA_TSE.1	TOE session establishment	CC	✓	✓	✓	✓		

Table 1 – Security Functional Requirements for the TOE

Key: (**D**)efined in (**PP**) , (**CC**) Part 2, (**A**)ssignment, (**S**)election, (**R**)efinement, (**I**)teration

6.1.1 Security audit (FAU)

6.1.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the minimum level of audit listed in **Table 2 – TOE auditable events;** and

c) Start-up and shutdown of the DBMS;

d) Use of special permissions (e.g., those often used by authorized administrators to circumvent access control policies); and

e) *"no additional events"*.

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, information specified in **the "Details" column of Table 2 – TOE auditable events**, below.

Security Functional Requirement	Auditable Event(s)	Details
FAU_GEN.1	None	None: SMF type 81 record (RACF initialization).
FAU_GEN.2	None	None
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	The identity of the authorized administrator that made the change to the audit configuration: DB2 audit trace audit class 3. SMF record type 102, IFCID 0142, IFCID 0106. DSN1SMFP can be used to report on these records.
FDP_ACC.1	None	None

Security Functional Requirement	Auditable Event(s)	Details
FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP	The identity of the subject performing the operation: DB2 audit trace classes 3, 4 and 5 for audited tables. SMF record type 102, IFCIDs 0142, 0143, 0144 and 0350 as well as utility IFCIDs 0023, 0024 and 0025. DSN1SMFP can be used to report on these records.
FDP_RIP.1	None	None
FIA_ATD.1	None	None
FIA_UAU.1	Unsuccessful use of the authentication mechanism	None: SMF type 80 record, event code 1, various qualifiers and SMF record type 30 subtypes 1 and 5. Covered by z/OS/RACF. In the case of a user authentication using DRDA, RACF is called for authentication.
FIA_UID.1	Unsuccessful use of the user identification mechanism, including the user identity provided	None: SMF type 80 record, event code 1, various qualifiers. Also, SMF type 30 record. Covered by z/OS RACF. In the case of a user authentication using DRDA, RACF is called for authentication.
FIA_USB_(EXT).2	Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject)	None: SMF type 80 record, event code 1, various qualifiers. Also, SMF type 30 record, subtypes 1 and 5. Covered by z/OS/RACF. In the case of a user authentication using DRDA, RACF is called for authentication.
FMT_MOF.1	None	None
FMT_MSA.1	None	None
FMT_MSA.3	None	None

Security Functional Requirement	Auditable Event(s)	Details
FMT_MTD.1	None	None
FMT_REV.1(1)	Unsuccessful revocation of security attributes	Identity of individual attempting to revoke security attributes: SMF type 80 record (generated by the RACF commands).
FMT_REV.1(2)	Unsuccessful revocation of security attributes	Identity of individual attempting to revoke security attributes: SMF type 80 record (generated by the RACF commands).
FMT_SMF.1	Use of the management functions	Identity of the administrator performing these functions: SMF type 80 record (generated by the RACF commands).
FMT_SMR.1	Modifications to the group of users that are part of a role	Identity of authorized administrator modifying the role definition: SMF type 80 record (generated by the RACF commands).
FPT_TRC.1	Restoring consistency	None: The TOE does not support DB2 data replication.
FTA_MCS.1	Rejection of a new session based on the limitation of multiple concurrent sessions	None: SMF type 80 record, event code 1, various qualifiers and SMF record type 30 subtypes 1 and 5.
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism	Identity of the individual attempting to establish a session: SMF type 80 record, event code 1, various qualifiers and SMF record type 30 subtypes 1 and 5.

Table 2 – TOE auditable events

Application note: This SFR includes also audit events collected in the audit trace maintained by DB2. The term “audit trace” is used instead of “audit trail” since this is the term used in the DB2 documentation. The requirement therefore covers only those events that are considered to be security relevant and are kept in the DB2 audit trace. Events that are addressed by the z/OS/RACF auditing are marked as such in the table and covered by the z/OS auditing functions even if the objects are DB2 objects. They are audited by RACF, not by DB2. Since the DB2 audit trace writes its records also into the SMF data sets using the functions of the z/OS SMF component, the requirements related to the management of the audit trail and the evaluation of the audit records are satisfied for the z/OS and the DB2 related audit records using the same functions.

Note 1: Exporting of information from the database is controlled by the access control functions of the operating system.

Note 2: When DB2 calls RACF for authenticating users that connect using the DRDA interface, it needs to be ensured that RACF is called in way that generates an audit record for every successful authentication attempt. Unsuccessful authentication attempts can be reported by using the DSN1SMFP utility.

Note 3: The DB2 administrative roles INSTALL SYSOPR and INSTALL SYSADM are used only during the installation process of the TOE and are deactivated once the TOE is properly installed. Those roles are therefore not covered by the audit requirements for FMT_SMR.1.

6.1.1.2 FAU_GEN.2 User identity association

FAU_GEN.2.1

For audit events resulting from actions of identified users and any identified groups, the TSF shall be able to associate each auditable event with the identity of the *user and group* that caused the event.

Application note: This SFR covers the user identity association that is specific to the DB2 audit trail.

6.1.1.3 FAU_SEL.1 Selective audit

FAU_SEL.1.1

The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) object identity;

c) user identity;

d) *no other identities*;

e) event type;

f) success of auditable security events;

g) failure of auditable security events;

h) audit level for table name; and

i) [audit policy, consisting of:

- *audit category,*
- *schema name,*
- *object type]*

Application note: This SFR covers the selective audit that is specific to the DB2 audit trail.

6.1.2 User data protection (FDP)

6.1.2.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1

The TSF shall enforce the Discretionary Access Control policy to objects on all subjects, all DBMS-controlled objects, and all operations among them.

6.1.2.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1

The TSF shall enforce the Discretionary Access Control policy to objects on the following [
Under the control of RACF:

a) The following access control attributes associated with a DB2 subject:
  - The primary DB2 authorization ID of the subject based on:
    i. User's RACF identity;
    ii. Group membership(s).
  - The TRUSTED, PRIVILEGED and RESTRICTED attributes of the user.

b) The following access control attributes associated with a RACF controlled DB2 object:
  - The subject's RACF access authority in the RACF access control list for the RACF profile protecting the RACF controlled DB2 privilege the user is using to access the RACF controlled DB2 object. Note that this includes access to RACF controlled DB2 privileges for RACF controlled DB2 administrative authorities;
  - The ownership (by a user or a database role) of the DB2 object.

Under the control of DB2:

c) The trusted context established by a DB2 subject and the following access control attributes associated with the related trusted context:
  - The primary DB2 authorization ID of the subject based on:
    i. The database role(s)

d) Access control rules for rows associated with a table based on the following attributes:
  - row permissions.

e) Transformation rules for a column associated with a table column based on the following attributes:
  - column mask.

].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
The Discretionary Access Control must result in granting access to an operation requested by a user (as defined by the primary DB2 authorization ID) on a DB2 object if:

- the access is granted by the implicit rights of a RACF controlled DB2 administrative authority or RACF controlled DB2 privilege and the user has that authority

or

- the user is the owner of the RACF controlled DB2 object and the requested privilege is granted to the owner of the DB2 object

or

- the user has established a trusted context with a database role assigned, the database role is the owner of the RACF controlled DB2 object and the requested RACF controlled DB2 privilege is granted to the owner of the object

or

- if the user is granted sufficient access by the following algorithm (note that this algorithm covers RACF controlled objects and permissions only):
  a) If the user has sufficient access authority in the standard access list of the RACF profile protecting the requested authority to the DB2 object, access is granted;

  b) If the user has sufficient access authority in the standard access list of the RACF profile protecting any type of DB2 privilege that allows access (according to the description in sections 7.3.4.1 to 7.3.4.19), access is granted;

  c) If the user has sufficient the TRUSTED or PRIVILEGED attribute, access is granted;

  d) If the current group of the user has sufficient access authority in the standard access list of the RACF profile protecting the requested authority to the DB2 object, access is granted;

  e) If the current group of the user has sufficient access authority in the standard access list of the RACF profile protecting any type of DB2 privilege that allows access (according to the description in sections 7.3.4.1 to 7.3.4.19), access is granted;

  f) If list-of-groups processing is in effect and the user is a member of a group that has sufficient authority in the standard access list of the RACF profile protecting the requested authority to the DB2 object, access is granted;

  g) If list-of-groups processing is in effect and the user is a member of a group that has sufficient access authority in the standard access list of the RACF profile protecting any type of DB2 privilege that allows access (according to the description in sections 7.3.4.1 to 7.3.4.20), access is granted;

  h) If a user ID of “*” is found on the standard access list of the RACF profile protecting the requested authority with sufficient authority and the current user is defined to RACF without the RESTRICTED attribute, access is granted;

  i) If a user ID of “*” is found on the standard access list of the RACF profile protecting any type of DB2 privilege that allows access (according to the description in sections 7.3.4.1 to 7.3.4.20) provides sufficient access and the current user is defined to RACF without the RESTRICTED attribute, access is granted;

  j) If the universal access authority (UACC) for the resource provides sufficient access authority (see Note) and the requesting user is not defined with the RESTRICTED attribute, access is granted;

  k) If the universal access authority (UACC) for the RACF profile protecting any type of DB2 privilege that allows access (according to the description in sections 7.3.4.1 to 7.3.4.20) provides sufficient access and the current user is defined to RACF without the RESTRICTED attribute, access is granted;

  l) RACF checks the user’s access authority in the conditional access list specified with WHEN(TERMINAL), WHEN(CONSOLE), WHEN(APPCPORT), WHEN(JESINPUT) or WHEN(SERVAUTH). If the user is in the list, if the user meets the specified condition (such as logged on at the specified terminal), and if the specified access authority is sufficient to allow access, access is granted;

  m) RACF determines whether the user has access to the resource because the user is a member of a group that meets a condition specified on the conditional access list specified with WHEN(TERMINAL), WHEN(CONSOLE), WHEN(APPCPORT), WHEN(JESINPUT) or WHEN(SERVAUTH) (AC.4-DB2-14). Which group is used depends on whether list-of-groups processing is in effect. RACF determines which group to use according to the following rules:

- If list-of-groups processing is not in effect, RACF uses only the user's current connect group;
- If list-of-groups processing is in effect, RACF finds all of the groups to which the user is connected that are also in the access list. Of these groups, RACF uses the group that has the highest access authority to the resource;
- If the group to be used according to the preceding rules has sufficient access authority to allow the requested access (see Note), access is granted;

n) If a user ID of "*" is found on the conditional access list specified with WHEN(TERMINAL), WHEN(CONSOLE), WHEN(APPCPORT), WHEN(JESINPUT) or WHEN(SERVAUTH), and if the current user is defined to RACF without the RESTRICTED attribute, and if the current user meets the specified condition (such as logged on at the specified terminal), and the access authority granted to * is sufficient to allow the requested access, access is granted;

o) RACF checks the user's access authority in the conditional access list specified with WHEN(PROGRAM). If the user is in the list, if the user meets the specified condition (such as running the specified program), and if the specified access authority is sufficient to allow access, access is granted;

p) If none of those conditions has granted access, access is denied;

and, if access is granted by the above algorithm, the following is evaluated:

- when a table has row access control activated and has one or more row permissions associated, then access to a table row is allowed if the row meets the WHERE search condition defined in at least one of the row permissions.
- when a table has column access control activated and the column has a column mask associated, then access to a column value is allowed after applying the CASE expression defined in the table column.

]

Application note 1: The terminology used in the rules described above corresponds to z/OS and RACF, which differ a bit from the one used in DB2:

a) User roles for security management are known in DB2 as "Administrative Authorities". Each administrative authority possess a set of privileges used in the TOE for enforcing the DAC policy. SYSADM is an example of an administrative authority considered for modeling the SFR as a user role (see FMT_SMR.1).

b) Privileges are granted to subjects and administrative authorities (user roles) and allow to define the access rules for each operation (e.g. in order to create a table, a subject must have the CREATE privilege; in order to truncate it, a subject must have the UPDATE privilege). A subject is allowed to perform a given operation on a DB2 object (e.g. execute an SQL statement on a table) only if the subject is granted with the specific privileges required by the operation. The set of access rules (based on privileges, administrative authorities and/or ownership) for an operation are determined by DB2.

c) The term ”database role” is used as a synonym for the DB2 “role” object. A database role can own a DB2 object and can be defined in trusted contexts for enforcing the DAC policy in a trusted context.

Application note 2: Sufficient access for RACF controlled DB2 objects means that a user with at least **READ** authorization to the RACF profile has sufficient access.

Application note 3: Additional technical details on the Discretionary Access Control policy are provided in section 7.3.3.

Application note 4: The concept of DB2 object ownership is laid out in section 7.3.3.2.

Application note 5: It should be noted that determining if an operation among controlled subjects and controlled objects is allowed is a synonym for determining the access authority of a controlled subject over a controlled object.

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [

a) if the user has the TRUSTED attribute, RACF grants the request.

b) If the user has the PRIVILEGED attribute, RACF grants the request.

]

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [

a) When a table has row access control activated and the table has no row permissions associated, then access to table rows is denied.

].

6.1.2.3 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to the following objects: [memory objects].

Application note: The evaluated parts of DB2 execute in their own address spaces. Object reuse of memory objects within those address spaces is provided by z/OS functions.
DB2 manages its own objects. When a DB2 object is deleted, DB2 ensures that the space that has been occupied by that object cannot be accessed by DB2 unless the space is allocated to another DB2 object and completely filled with the initial values for the new object. This ensures that values that are stored in space that is allocated to DB2 objects that have been deleted cannot be accessed by DB2 until the space is allocated to another DB2 object and has been prepared for reuse as part of the allocation.
DB2 stores its objects in z/OS data sets. Object reuse for data sets is provided by z/OS. RACF access control functions for data sets prohibit direct access by untrusted users to the data sets that are used by DB2

6.1.3 Identification and authentication (FIA)

6.1.3.1 FIA_ATD.1 User attribute definition

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users:

b) Database user identifier and ~~any~~ associated group memberships;

c) Security-relevant database roles **(DB2 privilege or DB2 administration authorities)**; and

[

c) TRUSTED, PRIVILEGE and RESTRICTED user attributes

d) other not relevant attributes

].

]

Application note 1: Item b) in this SFR has been refined to avoid confusion between the concept of role in DB2 (an object that can take ownership on a DB2 object and is part of the DAC policy in trusted contexts) and the concept of user role defined in CC. This difference is further explained in FMT_SMR.1.

Application note 2: User attributes are stored in RACF profiles.

6.1.3.2 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1

The TSF shall allow [no TSF mediated actions] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on the behalf of that user.

6.1.3.3 FIA_UID.1 User identification before any action

FIA_UID.1.1

The TSF shall allow [no TSF mediated actions] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on the behalf of that user.

6.1.3.4 FIA_USB_(EXT).2 Enhanced user-subject binding

FIA_USB_(EXT).2.1

The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [

a) The user identity that is associated with auditable events;

b) The user identity (or identities) and their user attributes used to enforce the Discretionary Access Control policy;

c) The group membership or memberships used to enforce the Discretionary Access Control policy;

d) The DB2 primary authorization ID;

e) In a trusted context, the database role defined by the trusted context, either globally or for the specific user identity (database role is optional or may not exist for the user identity).

]

Application note: A trusted context is established based upon the rules described in section 7.2.3.

FIA_USB_(EXT).2.2

The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of a user: [

a) A started task executes with the user ID defined in the STARTED RACF class or RACF started procedures table (ICHRIN03).

b) The primary DB2 authorization ID is initialized when the user makes a connection request. A DB2 agent structure is created to represent the user request that executes with the ID of the requesting user.

]

FIA_USB_(EXT).2.3

The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of a user: [

a) If a trusted context is established, this trusted context can:

- change the primary DB2 authorization ID,
- assign a database role.

]

Application note: DB2 supports a secondary authorization ID, an SQL ID and a RACF ID in addition to the primary authorization ID. In the evaluated configuration all those are identical to the value of the primary authorization ID, which is the RACF user ID.

FIA_USB_(EXT).2.4

The TSF shall enforce the following rules for the assignment of subject security attributes not derived from user security attributes when a subject is created: [none].

6.1.4 Security management (FMT)

6.1.4.1 FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1

The TSF shall restrict the ability to disable and enable the functions relating to the specification of events to be audited to authorized administrators.

6.1.4.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1

The TSF shall enforce the Discretionary Access Control policy to restrict the ability to manage all the security attributes to authorized administrators.

6.1.4.3 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1

The TSF shall enforce the Discretionary Access Control policy to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow no user to specify alternative initial values to override the default values when an object or information is created.

6.1.4.4 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1

The TSF shall restrict the ability to include or exclude the auditable events to authorized administrators.

Application note: This SFR covers the management of TSF data that is specific to the DB2 audit trail.

6.1.4.5 FMT_REV.1(1) Revocation (Users)

FMT_REV.1.1(1)

The TSF shall restrict the ability to revoke [user attributes] associated with the users under the control of the TSF to the authorized administrator.

FMT_REV.1.2(1)

The TSF shall enforce the rules [

a) The enforcement of the revocation of user security attributes stored in the user profile with the next user-subject binding process during the next authentication of the user;

b) the immediate revocation of security-relevant access authorization (active with the next access check being made).

]

6.1.4.6 FMT_REV.1(2) Revocation (Objects)

FMT_REV.1.1(2)

The TSF shall restrict the ability to revoke [object attributes] associated with the objects under the control of the TSF to the authorized administrator and database users with sufficient privileges as allowed by the Discretionary Access Control policy.

FMT_REV.1.2(2)

The TSF shall enforce the rules [

a) The required access authority associated with an object shall be enforced when an access check is made

]

6.1.4.7 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: [

a) manage RACF users and groups as well as their attributes;

b) manage access control to RACF controlled DB2 objects;

c) creation and deletion of database roles;

d) creation, modification and deletion of trusted contexts;

e) creation, modification and deletion of row permissions;

f) activation and deactivation of row access control;

g) creation, modification and deletion of column masks;

h) activation and deactivation of column access control;

i) creation, modification and deletion of audit policies;

j) configuration of audit level on tables.

]

Application note: Related to b), it should be noted that the *SEPARATE_SECURITY* DB2 system parameter can influence access control decisions as described in sections 7.3.4.1 to 7.3.4.20.

6.1.4.8 FMT_SMR.1 Security roles

FMT_SMR.1.1

The TSF shall maintain the user roles authorized administrator and [

a) users authorized by the discretionary access control policy to modify object security attributes;

b) DB2 System Administrator (SYSADM)

c) DB2 System Controller (SYSCTRL)

d) DB2 System Operator (SYSOPR)

e) DB2 Security administration (SECADM)

f) DB2 System Database Administrator (System DBADM or SYSDBADM)

g) DB2 Data Access (DATAACCESS)

h) DB2 Access Control (ACCESSCTRL)

i) DB2 Installation System Administrator (Install SYSADM)

j) DB2 Installation System Operator (Install SYSOPR)

k) DB2 Database Administrator (DBADM)

l) DB2 Database Controller (DBCTRL)

m) DB2 Database Maintainer (DBMAINT)

n) DB2 SQL Administrator (SQLADM)

o) DB2 Package Administrator (PACKADM)

]

Application note: In DB2, the "authorized administrator" is specified by the following roles: either SYSADM, Install SYSADM and Install SYSOPR or it is a combination of the listed administrators. In RACF the “authorized administrator” is defined as a user who is permitted by RACF to carry out administrative actions as defined by FMT_SMF.1.

FMT_SMR.1.2

The TSF shall be able to associate users with **user** roles.

Application note: In this requirement the term “role” is refined as “user role” to eliminate the ambiguity with the concept of role as defined in DB2. Whereas a security management role is known in DB2 with the term “administrative authority”, DB2 uses the term “role” or “database role” for a DB2 object that can own DB2 objects and be part of the DAC policy in trusted contexts.

6.1.5 Protection of the TSF (FPT)

6.1.5.1 FPT_TRC.1 Internal TSF consistency

FPT_TRC.1.1

The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2

When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [any database object].

Application note: The TOE does not contain physically separated components. Also, replication is not supported.

6.1.6 TOE Access (FTA)

6.1.6.1 FTA_MCS.1 Basic limitation on multiple concurrent sessions

FTA_MCS.1.1

The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2

The TSF shall enforce, by default, a limit of [2000] sessions per user.

6.1.6.2 FTA_TSE.1 TOE session establishment

FTA_TSE.1.1

The TSF shall be able to deny session establishment based on attributes that can be set explicitly by authorized administrator(s), including user identity and *group identity*, *time of day, day of the week*.

6.2 Security Functional Requirements Rationale

This section provides the rationale for the internal consistency and completeness of the security functional requirements defined in this Security Target.

6.2.1 Coverage

The following table shows that each security functional requirement defined in this ST addresses at least one security objective.

Name	Title	Objectives
FAU_GEN.1	Audit data generation	O.AUDIT_GENERATION
FAU_GEN.2, FAU_GEN.2	User identity association	O.AUDIT_GENERATION
FAU_SEL.1, FAU_GEN.1	Selective audit	O.AUDIT_GENERATION

Name	Title	Objectives
FDP_ACC.1	Subset access control	O.DISCRETIONARY_ACCESS O.MEDIATE O.TOE_ACCESS
FDP_ACF.1	Security attribute based access control	O.DISCRETIONARY_ACCESS O.MEDIATE O.TOE_ACCESS
FDP_RIP.1	Subset residual information protection	O.RESIDUAL_INFORMATION
FIA_ATD.1	User attribute definition	O.I&A O.TOE_ACCESS
FIA_UAU.1	Timing of authentication	O.I&A
FIA_UID.1	Timing of identification	O.I&A
FIA_USB_(EXT).2	Enhanced user subject binding	O.I&A
FMT_MOF.1	Management of security functions behavior	O.MANAGE
FMT_MSA.1	Management of object security attributes	O.MANAGE
FMT_MSA.3	Static attribute initialization	O.MANAGE
FMT_MTD.1	Management of TSF data	O.MANAGE
FMT_REV.1(1)	Revocation (user attributes)	O.MANAGE
FMT_REV.1(2)	Revocation (subject, object attributes)	O.MANAGE
FMT_SMF.1	Specification of Management Functions	O.MANAGE
FMT_SMR.1	Security roles	O.ADMIN_ROLE O.MANAGE
FPT_TRC.1	Internal TSF consistency	O.MEDIATE
FTA_MCS.1	Basic limitation on multiple concurrent sessions	O.TOE_ACCESS
FTA_TSE.1	TOE session establishment	O.TOE_ACCESS

Table 3 – Mapping between SFRs and Security Objectives

6.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements defined in this ST are suitable to meet and achieve the security objectives.

Security Objectives	SFRs	Rationale
O.ADMIN_ROLE	FMT_SMR.1	The TOE will establish, at least, an authorized administrator role. The ST writer may choose to specify more roles. The authorized administrator will be given privileges to perform certain tasks that other users will not be able to perform. These privileges include, but are not limited to, access to audit information and security functions as required in FMT_SMR.1

Security Objectives	SFRs	Rationale
O.AUDIT_GENERATION	FAU_GEN.1 FAU_GEN.2 FAU_SEL.1	The events to be audited in DB2 are defined in FAU_GEN.1 and are associated with the identity of the user that caused the event FAU_GEN.2 for the audit trail that is resulting from RACF actions and FAU_GEN.2 for the DB2 audit trail. The TOE supports a selection of which events may be audited based on a set of attributes. (FAU_SEL.1 for the audit trail that is resulting from RACF actions and FAU_GEN.2 for the DB2 audit trail). The date and time used in the audit records and upon which FAU_GEN.1 has a dependency that is assumed to be provided by the operating system or the underlying platform.
O.DISCRETIONARY.ACCESS	FDP_ACC.1 FDP_ACF.1	The TSF must control access of subjects and/or users to named resources based on identity of the object, subject, or user. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode. The access control policy has a defined scope of control as required by FDP_ACC.1. The rules for the access control policy are defined in FDP_ACF.1.
O.I&A	FIA_ATD.1 FIA_UID.1 FIA_UAU.1 FIA_USB_(EXT).2	The TSF ensure that only authorized users gain access to the TOE and its resources. Users authorized to access the TOE must use an identification and authentication process as required FIA_UID.1 and FIA_UAU.1. To ensure that the security attributes used to determine access are defined and available to the support of authentication decisions as required by FIA_ATD.1. Proper authorization for subjects acting on behalf of users is also required by FIA_USB_(EXT).2 .
O.MANAGE	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_REV.1(1) FMT_REV.1(2) FMT_SMF.1 FMT_SMR.1	FMT_MOF.1 requires that the ability to use particular TOE capabilities be restricted to the administrator. FMT_MSA.1 requires that the ability to perform operations on security attributes be restricted to particular roles. FMT_MSA.3 requires that default values used for security attributes are restrictive. FMT_MTD.1 requires that the ability to manipulate TOE content is restricted to administrators. FMT_REV.1 restricts the ability to revoke attributes to the administrator.

Security Objectives	SFRs	Rationale
		FMT_SMF.1 identifies the management functions that are available to the authorized administrator. FMT_SMR.1 defines the specific security roles to be supported.
O.MEDIATE	FDP_ACC.1 FDP_ACF.1 FPT_TRC.1	The FDP requirements were chosen to define the policies, the subjects, objects, and operations for how and when mediation takes place in the TOE. FDP_ACC.1 defines the Access Control policy that will be enforced on a list of subjects acting on the behalf of users attempting to gain access to a list of named objects. All the operations between subject and object covered are defined by the TOE's policy. FDP_ACF.1 defines the security attribute used to provide access control to objects based on the TOE's access control policy. FPT_TRC.1 ensures replicated TSF data that specifies attributes for access control must be consistent across distributed components of the TOE. The requirement is to maintain consistency of replicated TSF data. *(Please note that the TOE does not support replication)*
O.RESIDUAL_INFORMATION	FDP_RIP.1	FDP_RIP.1 is used to ensure that when a DB2 object is deleted, the space that has been occupied by those objects cannot be accessed by TOE functions unless the space is allocated to another DB2 object and completely filled with the initial values for this new object.
O.TOE_ACCESS	FDP_ACC.1 FDP_ACF.1 FIA_ATD.1 FTA_MCS.1 FTA_TSE.1	FDP_ACC.1 requires that each identified access control SFP be in place for a subset of the possible operations on a subset of the objects in the TOE. FDP_ACF.1 allows the TSF to enforce access based upon security attributes and named groups of attributes. Furthermore, the TSF may have the ability to explicitly authorize or deny access to an object based upon security attributes. FIA_ATD.1 defines the security attributes for individual users including the user's identifier and any associated group memberships. Security relevant roles and other identity security attributes. FTA_MCS.1 ensures that users may only have a maximum of a specified number of active sessions open at any given time. FTA_TSE.1 allows the TOE to restrict access to the TOE based on certain criteria.

Table 4 – Security objectives for the TOE rationale

6.2.3 Security Requirements Dependency Analysis

Please refer to [DBMSPP], section 8.3.3 for this analysis.

6.3 TOE security assurance requirements

The security assurance requirements for the TOE correspond to Evaluation Assurance Level 4, augmented by ALC_FLR.3, as specified in [CC] part 3. As the security assurance requirements are extremely well defined in [CC] part 3, the ST author sees no need to list them in this document again, more so as no augmentations to the assurance requirements are acutally intended, hence: EAL 4.

6.4 Security Assurance Requirements Rationale

The evaluation assurance level (EAL) has been considered appropriate for a well-controlled, non-hostile environment and has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE. Additionally, the evaluation assurance level is consistent with the minimum assurance level (EAL 2) stated in [DBMSPP].

6.5 TOE Summary Specifications Rationale

6.5.1 Security functions justification

The following table maps the security functional requirements to the security functions as defined in the TOE summary specification to show that all security functional requirements are addressed by the security functions.

SFR	Security Functions
FAU_GEN.1	Section 7.5 explains how the TOE generates records. This section also explains the structure of the audit records.
FAU_GEN.2	Section 7.5 explains the context information the TOE generates in the audit records. It also explains the information contained in the audit records.
FAU_SEL.1	Section 7.5 explains how system and database administrators can configure the events that are audited through the use of audit policies and specifying audit at table level. Sections 7.4.1 explains the auditor role which can configure the events that are audited using the RACF commands.
FDP_ACC.1	The general operation of access control for DB2 is explained in Section 7.3, with the principles being explained in section 7.3.1. The administrative authorities for DB2 are explained in section 7.3 and the privileges for the different DB2 objects are explained in sections 7.3.3.
FDP_ACF.1	Section 7.3.3ff explains the access control for DB2 objects.
FDP_RIP.1	Object reuse for DB2 objects is described in section 7.6.
FIA_ATD.1	Section 7.2 describes the concept of trusted context associated with a user, section 7.3.3 explains the concept of administrative authorities (user roles) in DB2; other user attributes are also used in RACF and are described in section 7.4.1.1.
FIA_UAU.1	User authentication to DB2 is explained in section 7.2.

SFR	Security Functions
FIA_UID.1	User identification is explained in section 7.2.1.
FIA_USB_(EXT).2	User subject binding for trusted contexts in DB2 is explained in section 7.2.2ff.
FMT_MOF.1	Section 7.5.3 and describe management of auditing.
FMT_MSA.1	Management of object security attributes is explained in sections 7.4.2ff.
FMT_MSA.3	DB2 security management is explained in section 7.4.1ff Default values for the access control are defined in the UACC attribute in the resource profiles as explained in section 7.4.1.2 in the description of the resource profiles.
FMT_MTD.1	Audit event management is explained in sections 7.5.
FMT_REV.1(1)	Revocation of object security attributes is explained in section 7.4.1 of for the management of general resource profiles.
FMT_REV.1(2)	Revocation of user security attributes is explained in section 7.4.1.
FMT_SMF.1	Security management functions in DB2 are described in section 7.4,2ff.
FMT_SMR.1	DB2 user roles (known as administrative authorities in DB2) are explained in sections 7.3 and 7.4.
FPT_TRC.1	The TOE does not support replication, thus the data are always held on one physical system.
FTA_MCS.1	Section 7.2.4 describes how DB2 and RACF limit the number of sessions.
FTA_TSE.1	Section 7.2 describes the condition under which the access to the TOE can be granted.

Table 5 – Mapping of security functional requirements to security functions

7 TOE summary specification

This chapter provides a summary description of the security functions of the TOE.

The TOE builds upon the security functionality already available in the z/OS platform (see subsections of chapter 6, “TOE summary specification” of [ZOSST]). Please refer to [ZOSST] for the functionality of the z/OS software platform; the security functionality of DB2 is described in the following sub-sections. Security claims are defined in this chapter in the form (XX.n-DB2-m)

7.1 Overview of the TOE

The TOE is the combination of DB2 and RACF. The TOE is operating on top of z/OS and z/OS is an operating system that runs on the IBM z/Architecture processors. Those processors provide separate problem and supervisor states as well as memory protection functions that allow z/OS to prohibit direct access from untrusted applications to I/O devices, protected memory areas used by the TOE, and memory areas used by other applications. Using these processor functions, the z/OS operating system provides the capability for applications to execute in separate and protected address spaces and the TOE uses this capability to establish a set of domains for its own execution that is protected from direct access by untrusted applications.

The underlying firmware also allows the definition of separate logical partitions where several instances of the TOE can execute in parallel on the same hardware. The TOE may also be loaded in one logical partition while other non-TOE software is loaded in other logical partitions. The logical partitioning function is part of the TOE environment and has been evaluated separately.

The TOE provides an interface to applications by allowing them to request TOE services.

The TOE provides the following security functions:

1. Identification and authentication
2. Discretionary access control based on access control lists associated with objects
3. Management functions to administer auditing, discretionary access control as well as users and groups with their related attributes
4. An audit trail for security relevant events
5. Object reuse

z/OS, the base operating system itself is logically structured into the following major units:

1. The Hardware Configuration Definition (HCD), which mirrors the IOCDS definition of the logical partitioning system (PR/SM)
2. The Base Control Program (BCP), which is responsible for handling supervisor call interrupts, program call interrupts, and all other interrupts, and task scheduling and memory management, including the management of address spaces
3. The Data Facility Storage Management Subsystem (DFSMS), which is responsible for accessing and managing disk and tape devices, including the data sets on those devices
4. The Communication Server, which is responsible for network communication using SNA- or IP-based protocols
5. The Job Entry Subsystem (JES2), which is responsible for scheduling jobs and handling spool files (for the purpose of the evaluation, the SDSF display facility is considered to be part of JES2)
6. The UNIX System Services, which provides UNIX programming and user interfaces
7. The Resource Access Control Facility (RACF), which is the central system for discretionary and mandatory access control to resources (**which is part of the TOE**).

8. The Time Sharing Option Extensions (TSO/E) system, which is responsible for handling of commands issued by users at TSO/E terminals

The TOE itself consists of a set of “nuclei” operating in the supervisor state of the underlying abstract machine and a set of “trusted processes” that either also operate in supervisor state or operate as “authorized programs”. Those authorized programs start their operation in problem state, but can switch into supervisor state, operate with storage key 0, or both, so are therefore not limited in their capabilities by any element of the system security policy.

The TOE thus operates as a set of "trusted processes" on top of z/OS.

7.1.1 DB2 Structure and Architecture

DB2 operates as a subsystem of z/OS. DB2 provides a set of external interfaces that can be called by "attachment facilities". Those attachment facilities are library interfaces that call the DB2 services using protected interfaces registered to z/OS. Those interfaces extend the interfaces of z/OS with services implemented in the DB2 address spaces.

User programs can further request services from the DB2 subsystem using the Program Call (PC) instruction with function codes assigned to DB2. DB2 accepts those requests after the user has been "connected" to DB2 and successfully identified. DB2 then creates an "agent structure" for the user's address space. The user's address space,represented by that agent structure, can then request general services and DB2 (executing in its own protected address spaces) will check the user's permission to those services before performing the service

In addition, DB2 provides an interface for external users that allows access DB2 objects. This external interface implements the Distributed Relational Database Architecture (DRDA) and the Distributed Data Management commands.

DB2 uses RACF to identify and authenticate users as well as for the management and enforcement of access rights to DB2 objects. DB2 has its own set of classes defined within RACF where individual profiles represent the individual DB2 objects and authorities to those objects. DB2 also uses the auditing capabilities of RACF to audit (successful and/or attempted) access to DB2 objects.

The DB2 part of the TOE is structured into the following major units:

1. The System Services (DSCF) Address Space
2. The Database Services (ADMF) Address Space
3. The Distributed Data Facility Services (DDF) Address Space
4. The Internal Resource Lock Manager (IRLM) Address Space
5. The Attachment Facilities
6. The DB2 utilities

7.1.2 RACF Structure and Architecture

RACF is implemented as a dedicated component that can be used by operating system components and trusted applications to

- authenticate users
- control access to resources
- manage access rights
- manage users and groups with their security attributes
- log and report attempts to authenticate or access protected resources

RACF manages the information it relies on in its own database. This database includes user and group profiles, which store information about individual users and groups with the security attributes assigned to the users and groups. It also includes resource profiles, where those profiles represent the resources for which a resource manager can call RACF in order to check for a user's authority to access a specific resource. In addition, RACF manages access rights associated with resource profiles, which define the type of access users or groups have to the resource.

RACF has the capability to generate audit records for specific events. RACF also provides an interface to resource managers that they can use to cause RACF to generate a specific audit record. Audit records generated by RACF are not stored in the RACF database, but passed to the components of z/OS, which are centrally used to store and manage all types of audit records.

RACF has three main sets of interfaces:

- The RACROUTE macro interface, which sufficiently authorized programs executing within z/OS can use to request services from RACF
- The RACF callable services, which also sufficiently authorized programs executing within z/OS can use to request services from RACF. Those services include specific services related UNIX file systems and UNIX IPC objects.
- The RACF command interface which sufficiently authorized users can use to perform RACF management functions.

The authorizations required to use the function as at the interface are defined with the individual functions and may even be dependent on the parameters used.

7.2 Identification and authentication

7.2.1 Authentication function

A user can interact with the TOE in one of the following ways:

- As a TSO user
- As an operator at a console
- By submitting a job to be initiated and scheduled by the Job Entry Subsystem (JES2)
- As a UNIX user
- As a user connecting to the DRDA interface of DB2
- Through an external entity that establishes a trusted context, authorized by the association with a trusted context (see section 7.2.3)

In all cases, users are identified and authenticated by their credentials (IA.1.1) before being authorized to perform any other security relevant action. In the case of jobs submitted by an already-authenticated user, no additional authentication is required for jobs running with the ID of the user who submitted them. The internal reader accepts (and relies) in this case on the authentication performed when the user has logged on to TSO (IA.1.2).

RACF provides the capability to control who can log into the system based on days and time of access, thus allowing for control when the TOE can be accessed. Additionally, RACF administrators can control which user can access (logical) terminals and when (based on days and time of access) based on either individual users or groups (IA.4-DB2-TSE). See also section 7.4.1 for more information on the management of these controls.

Applications, such as DB2, requesting RACF to authenticate a user will usually also request RACF to create a specific control block, named Accessor Control Environment Element (ACEE). The content of the ACEE is built from information taken from the user's profile in the RACF database and from information provided by the application requesting authentication. Examples of information supplied by the requesting application are the "Port of entry" or the name of the application. The ACEE is later used in access checks performed by RACF when the user related information like the user's RACF attributes, group memberships, port of entry, etc. are evaluated as part of the access control algorithm.

7.2.2 Special handling in DB2

When a local user connects to DB2 using one of the attachment facilities, DB2 will use the RACF user ID of the user making the connection as the primary DB2 authorization ID (IA.4-DB2-*). In the evaluated configuration no secondary authorization ID will be defined and the SQL ID as well as the RACF ID will be identical to the primary DB2 authorization ID (IA.4-DB2-1).

Users connecting using the external DRDA interface are authenticated by RACF to validate the user's credentials and eventually will allow the user to perform any other action only after he has been successfully authenticated (IA.4-DB2-2).

7.2.3 Trusted contexts

Additionally, a user or user application can interact with the TOE through what is known as a “trusted context” or trusted connection. A trusted context, which can be local or remote, is established when the connection attributes match the attributes of a unique trusted context defined in the TOE.

For a local connection (IA.4-DB2-5), the TOE determines if can be trusted based on:

- A system authorization ID, which is the primary DB2 authorization ID used to establish the connection: the USER parameter included in the JOB statement (for BATCH or RRSAF), the RACF user id (for RRSAF) or the TSO logon ID (for TSO).
- The job or started task name

For a remote connection (IA.4-DB2-6), the TOE determines if that can be trusted based on:

- The system authorization ID which is determined either by a set of rules included in the SYSIBM catalog tables[1] (for z/OS requesters), derived from the authentication token (for z/OS servers[2]), or otherwise derived from the user id provided by the external entity (e.g. a middleware server).
- The following optional connection trust attributes:
  - The client IP address or domain name (ADDRESS)
  - The network access security zone name (SERVAUTH)
  - The minimum level of encryption of the data stream (ENCRYPTION)

Once the user or remote application is authenticated, access control can be based on a database role, a different user depending on the rules defined in the trusted context (IA.4-DB2-7).

7.2.4 Session Limits

DB2 uses the RACF custom field USER.CSDATA.DSNMUCTL associated with a primary DB2 authorization ID in RACF to determine the maximum number of simultaneous connections for a user. The maximum value for this field is 2000. DB2 validates that the session limit set for the user in RACF is not exceeded (IA.4-DB2-SL.1).

[1] For more information, see “Establishing remote trusted connections by DB2 for z/OS requesters” in the DB2 v12 for z/OS Managing Security.

[2] For more information, see “Establishing remote trusted connections to DB2 for z/OS servers” in the DB2 v12 for z/OS Managing Security.

7.3 Access control

7.3.1 Access control principles

The TOE comprises the Resource Access Control Facility (RACF) as the component that performs access control between subjects acting on behalf of a user and resources protected by the discretionary access control policies. RACF uses user and resource profiles it stores in the RACF database to decide if a subject has access to a non-UNIX resource like DB2 objects.

Access to DB2 objects is generally controlled by RACF. DB2 acts as a resource manager for those objects and calls RACF when a user attempts to access one of those objects. A set of DB2 specific classes are defined in RACF to model DB2 administrative authorities, DB2 privileges and DB2 objects, and profiles in those classes are used to protect the DB2 resources.

Access control is also implemented through trusted contexts, a new concept that has been developed to have a more precise control of security. The trusted context also determines how access control will be enforced. Once the trusted connection is authenticated, a role or a different user id can be assigned to the connection, depending on the rules defined by the trusted context:

- A role provides privileges, in addition to the current set of privileges that are granted to the primary and secondary authorization identifiers. A role can own objects if the objects are created in a trusted context with the role defined as the owner. If a role is defined as an owner, then only the privileges that are granted to the role are considered for object ownership.
- Assigning a different user to the trusted connection forces the discretionary access control using the access rights of the impersonated user.

7.3.1.1 The authorization hierarchy

Users (as identified by an authorization ID) can successfully execute DB2 commands, utilities or SQL statements only if they have the privilege to perform the specified operation. Access is controlled within DB2 by granting or revoking privileges and related authorities that can be assigned to an authorization IDs or role. The two forms of authorization are administrative authorities and privileges.

7.3.1.1.1 Privileges

A privilege enables its holder to perform a specific operation, sometimes on a specific object.

Privileges can be explicit or implicit. An explicit privilege is a specific type of privilege. Each explicit privilege has a name and is the result of either a GRANT statement or a REVOKE statement (not allowed in the evaluated configuration), or the assignment of the DB2 privilege to the user in the RACF database.

An implicit privilege comes from the ownership of objects, including plans and packages. For example, users are granted implicit privileges on objects that are referenced by a plan or package when they are authorized to execute the plan or package.

7.3.1.1.2 Administrative Authority

An administrative authority is an administration role that can be granted to users in order to perform administrative tasks on DB2.

Authorities often include privileges that are not explicit, have no name, and cannot be specifically granted. For example, when an ID is granted the SYSOPR administrative authority, the ID is implicitly granted the ability to terminate any utility job.

Administrative authorities fall into the categories of system, database, and collection authorities:

System authorities include:

SYSADM: System administration authority includes all DB2 privileges (except for a few that are reserved for installation), which are all grantable to others. In case the SEPARATE_SECURITY system parameter is set to NO, SYSADM can also create roles and trusted contexts, and grant and revoke privileges (not allowed in the evaluated configuration).

SYSCTRL: System control authority includes most SYSADM privileges; it excludes the privileges to read or change user data. In case the SEPARATE_SECURITY system parameter is set to NO, SYSCTRL can also create roles.

SYSOPR: System operator authority includes the privileges to issue most DB2 commands and end any utility job.

SECADM: Security administration authority that manages security related objects (row permissions, column masks, roles, trusted contexts, secured triggers and user-defined functions), creates audit policies, and grant and revoke privileges and authorities (not allowed in the evaluated configuration).

System DBADM or SYSDBADM: Database administration authority that allows the separation of object management from data access and granting of privileges. System DBADM can manage databases across a DB2 subsystem (i.e. create, alter and drop DB2 objects), while having no access to the data in the databases.

SQLADM: SQL administration authority provides the ability to monitor and tune SQL without any additional privileges.

DATAACCESS: Data access administrative authority that can access data in all user tables.

ACCESSCTRL: Access control administrative authority that does grants and revokes (not allowed in the evaluated configuration).

In addition, there are two authorities predefined in DB2 that are used for the installation and start-up of DB2. Those authorities need to be removed from any user once the TOE is fully set up:

Install SYSADM

Install SYSOPR

Database authorities (ranked from highest to lowest) include:

DBADM: Database administration authority includes the privileges to control a specific database. Users with DBADM authority can access tables and alter or drop table spaces, tables, or indexes in that database.

DBCTRL: Database control authority includes the privileges to control a specific database and run utilities that can change data in the database.

DBMAINT: Database maintenance authority includes the privileges to work with certain objects, and to issue certain utilities and commands in a specific database.

Collection authorities include:

PACKADM: Package Administrator has all privileges on all packages in specific collections and can create new packages in those collections.

Administrative authorities are considered in this ST as security management roles for modeling the security functional requirements.

In the evaluated configuration access control to DB2 objects is performed using RACF. Profiles are defined within RACF in DB2 specific classes and used by DB2 to perform access checking. A generic profile needs to be established in every class so that all access control is provided by RACF.

7.3.2 RACF-protected resources of DB2

The TOE provides the Resource Access Control Facility (RACF) as the component that performs access control between software running on behalf of a user and resources protected by the Discretionary and Mandatory access control policies. RACF uses user and resource profiles it stores in the RACF database to decide if a subject has access to a resource. In addition to RACF, DB2 for z/OS itself provides discretionary access control using the GRANT/REVOKE privileges. In the evaluated configuration those privileges will not be evaluated and therefore have no effect since all checks for DB2 objects mentioned in this Security Target will be performed by RACF.

DB2 for z/OS calls the RACF component using the internal interface to RACF to check the access rights of the user or role that initiated the user request and passes the ID of the user and user attributes like the name and type of the resource and the requested type of access to RACF.

RACF uses the ACEE (which represents the user's profile) and any role associated with the process, and retrieves the resource profile from its external database or the internal cache and checks if the user with his current security attributes is allowed to access the resource in the requested access mode.

RACF returns either a “yes” or a “no” decision for the access request in cases where the user and the resource are both known to RACF. If either of them is not known RACF returns a “don’t know” return code. In the latter case the resource manager needs to make its own decision whether to allow access or not, which in the DB2 case results into the use of the rights managed using the GRANT and REVOKE statements. Depending on the decision the resource manager will either perform or reject the access request of the user program. In the evaluated configuration of the TOE predefined generic profiles will ensure that RACF always finds a profile that matches the object and therefore RACF will always be able to make the access decision for the type of objects listed in this Security Target.

7.3.3 Discretionary access control in DB2

Note that rows are **not** objects that are subject to discretionary access control through RACF. Row and column access control provides additional discretionary access control on a finer granularity; see section 7.3.4.20 for additional detail.

7.3.3.1 DB2 objects

Discretionary access control to RACF resources is controlled by the user, groups and administrative authorities assigned to, database role, and resource profiles stored and managed by RACF. Role is only considered when a trusted context is established.

Access control is defined for DB2 objects, please refer to section 1.4.1.2.1 for an enumeration and hierarchy of relevant DB2 objects.

Ownership to a DB2 object can be assigned to a primary or secondary authorization ID (user ID and group ID in RACF, respectively) or a database role. In trusted contexts, role ownership in DB2 objects and the role assigned to the process based on the trusted context definition are taking into account in the Discretionary Access Control policy. In non-trusted contexts or connections, only authorization ID ownership is used.

Note that index access is controlled by the access to the table.

Each DB2 command, utility, and Structure Query Language (SQL) statement is associated with a set of privileges, administrative authorities, or both. Authority checking is performed with the support of the RACF access control module where DB2 authority checking uses RACF such that:

- DB2 object types map to RACF class names
- DB2 privileges map to RACF resource names for DB2 objects
- DB2 administration authorities map to the RACF administrative authority class (DSNADM) and RACF resource names for DB2 authorities
- DB2 security rules map to RACF profiles

The RACF access control module checks the RACF profiles corresponding to that set of privileges and authorities.

RACF has the following classes defined for DB2 objects:

• DSNADM	DB2 administrative authority class
• DSNR	Grouping and member classes for DB2 subsystems
• GDSNBP or MDSNBP	Grouping and member classes for DB2 buffer pool privileges
• GDSNCL or MDSNCL	Grouping and member classes for DB2 collection privileges

- GDSNDB or MDSNDB Grouping and member classes for DB2 database privileges
- GDSNJR or MDSNJR Grouping and member classes for DB2 Java archive files
- GDSNPK or MDSNPK Grouping and member classes for DB2 package privileges
- GDSNPN or MDSNPN Grouping and member classes for DB2 plan privileges
- GDSNSC or MDSNSC Grouping and member classes for DB2 schemas privileges
- GDSNSG or MDSNSG Grouping and member classes for DB2 storage group privileges
- GDSNSM or MDSNSM Grouping and member classes for DB2 system privileges
- GDSNSP or MDSNSP Grouping and member classes for DB2 stored procedure privileges
- GDSNSQ or MDSNSQ Grouping and member classes for DB2 sequences
- GDSNTB or MDSNTB Grouping and member classes for DB2 tables, index or view privileges
- GDSNTS or MDSNTS Grouping and member classes for DB2 table space privileges
- GDSNUF or MDSNUF Grouping and member classes for DB2 user-defined function privileges
- GDSNUT or MDSNUT Grouping and member classes for DB2 user-defined distinct type privileges
- GDSNGV or MDSNGV Grouping and member classes for DB2 global variables privileges

Note: There are no classes defined in RACF for row permission and column mask objects.

Profiles in those classes are defined using the following naming conventions:

- For a single-subsystem scope, the general format for a resource name (privilege name) is: *object-name.privilege-name*
- For a multiple-subsystem scope, the general format for a resource name (privilege name) is: *DB2-subsystem.object-name.privilege-name*

In most cases the resources protected by RACF are specific privileges. In the following section the resource names are for simplification always specified in the format for a multiple-subsystem scope.

The following table shows the DB2 objects and their associated object name qualifier in RACF profiles:

DB2 object	Object name qualifiers
Buffer pool	*bufferpool-name*
Collection	*collection-ID*
Database	*database-name*
Java archive (JAR)	*schema-name.JAR-name*
Package	*collection-ID.package-ID* *collection-ID* *owner*
Plan	*plan-name* *owner*
Role	not applicable

DB2 object	Object name qualifiers
Schema	*schema-name* *schema-name.function-name* *schema-name.procedure-name* *schema-name.type-name*
Sequence	*schema-name.sequence-name*
Storage group	*storage-groupname*
Stored procedure	*schema-name.procedure-name*
System	*owner*
Table, index	*table-qualifier.table-name* *table-qualifier.table-name.column-name*
Tablespace	*database-name.table-space-name*
Trusted context	not applicable
User-defined distinct type	*schema-name.type-name*
User-defined function	*schema-name.function-name*
View	*view-qualifier.view-name* *table-qualifier.table-name.view-qualifier.view-name* *table-qualifier.table-name.column-name.view-qualifier.view-name*
Global variable	*schema- name.variable-name*

Table 6 – Object name qualifiers in RACF profiles

Note 1: Java ARchive (JAR), user-defined distinct type and user-defined function are listed here for completeness. In the evaluated configuration no Java ARchives (JARs), distinct types or user-defined functions are included.

Note 2: The ‘system’ object in the above list is a construct used by RACF to map DB2 Administrator authorities and DB2 privileges to RACF profiles. There is no ‘system’ object in the object hierarchy within DB2.

As with all other RACF profiles the use of generic RACF profiles may simplify the management and administration of DB2 privileges significantly.

7.3.3.2 DB2 object ownership

When an object is created, one authorization ID is assigned ownership of the object. Ownership means that the user is authorized to reference the object in any applicable SQL statement. The privileges on the object can be granted by the owner, and cannot be revoked from the owner. Owners of views only receive the level of privileges that they have on the underlying table or view. The owner of the object that is being created is determined as follows (AC.4-DB2-OO.1):

- If the schema qualifier is not explicitly specified, the owner depends on how the CREATE statement is issued:
    - If the CREATE statement is embedded in a program, the owner of the object that is being created is the authorization ID that serves as the implicit qualifier for unqualified object names. This is the authorization ID that is in the QUALIFIER option when the plan, package, or native SQL procedure (that contains the CREATE statement) is created or last changed. If the QUALIFIER option is not used, the owner of the object is the authoriza-

    tion ID in the OWNER option when the plan, package, or native SQL procedure is created or last changed. If the OWNER option is not used, the owner is the owner of the plan, package, or native SQL procedure. If the plan or package was last bound in a trusted context that is defined with the ROLE AS OBJECT OWNER clause, a role is the owner.

    - If the CREATE statement is dynamically prepared, the owner of the object that is being created is the authorization ID of the process.
    - If the CREATE statement is execute in a trusted context that is defined with the ROLE AS OBJECT OWNER clause, the role of the primary authorization ID is the owner.

- If the schema qualifier is explicitly specified, the owner depends on the type of object that is being created unless the CREATE statement is executed in a trusted context that is defined with the ROLE AS OBJECT OWNER clause. When the CREATE statement is executed in a trusted context that is defined with the ROLE AS OBJECT OWNER clause, the owner of the object is determined as follows:
    - If the CREATE statement is embedded in a program, the role that owns the plan or package is the owner of the object.
    - If the CREATE statement is dynamically prepared, the primary authorization ID is the owner.
- If the schema qualifier is explicitly specified, and the CREATE statement is not executed in a trusted context that is defined with the ROLE AS OBJECT OWNER clause, the owner depends on the type of object that is being created:
    - For an alias, auxiliary table, created global temporary table, table, or view, the owner of the object that is being created is the same as the explicit schema name.
    - For a user-defined distinct type, user-defined function, procedure, sequence, JAR files, or trigger, the owner of the object that is being created is the authorization ID of the process.

The rules that determine ownership of row permissions and column masks are the same as those that determine ownership of objects like user-defined distinct types, user-defined functions, procedures, sequences, JAR files, or trigger.

Only users with SECADM or SYSADM authority (when SEPARATE_SECURITY parameter = "No") can manage and maintain row permissions and column masks (AC.4-DB2-OO.2).

7.3.4 Access evaluation algorithm for DB2 objects

In the evaluated configuration access to DB2 privileges is granted either because of the implicit privileges in a DB2 administration authority, because of implicit access rights of the owner of the object or because of RACF managed access rights. Those RACF managed access rights are defined via access control lists to the RACF profiles representing the DB2 privilege or DB2 administration authority to the DB2 object.

The algorithm described here for the evaluation of RACF controlled access rights to DB2 objects assumes that RACF is configured in accordance with the requirements of this Security Target, especially that:

1. RACF is active
2. All the resource classes listed in this Security Target for DB2 have been defined, are active and are RACLISTed
3. Appropriate generic profiles have been defined such that all DB2 privileges and DB2 administration authorities that can be RACF protected have at least a generic profile defined that protects them

In this case the following algorithm is used to evaluate the access right a user (as defined by the primary DB2 authorization ID) has to a DB2 privilege or DB2 administration authority to a DB2 object:

1. If the user has a specific DB2 administration authority, granted by the implicit rights of a RACF controlled administration authority, access is granted (AC.4-DB2-1)

2. If the user is the owner of the DB2 object and the requested DB2 administration authority is granted to the owner of the object, access is granted (AC.4-DB2-2a)
3. In a trusted context, if there is a database role assigned, the database role is the owner of the DB2 object and the requested DB2 administrative authority is granted to the owner of the object, access is granted (AC.4-DB2-2b)If the user has sufficient access authority in the standard access list of the RACF profile protecting the requested authority to the DB2 object, access is granted (AC.4-DB2-3).
4. If the user has sufficient access authority in the standard access list of the RACF profile protecting any type of DB2 privilege that allows access (according to the description in sections 7.3.4.1 to 7.3.4.19), access is granted (AC.4-DB2-4).
5. If the user has sufficient the TRUSTED or PRIVILEGED attribute, access is granted (AC.4-DB2-4b).
6. If the current group of the user has sufficient access authority in the standard access list of the RACF profile protecting the requested authority to the DB2 object, access is granted (AC.4-DB2-5).
7. If the current group of the user has sufficient access authority in the standard access list of the RACF profile protecting any type of DB2 privilege that allows access (according to the description in sections 7.3.4.1 to 7.3.4.19), access is granted (AC.4-DB2-6)
8. If list-of-groups processing is in effect and the user is a member of a group that has sufficient authority in the standard access list of the RACF profile protecting the requested authority to the DB2 object, access is granted (AC.4-DB2-7).
9. If list-of-groups processing is in effect and the user is a member of a group that has sufficient access authority in the standard access list of the RACF profile protecting any type of DB2 privilege that allows access (according to the description in sections 7.3.4.1 to 7.3.4.20), access is granted (AC.4-DB2-8)
10. If a user ID of “*” is found on the standard access list of the RACF profile protecting the requested authority with sufficient authority and the current user is defined to RACF without the RESTRICTED attribute, access is granted (AC.4-DB2-9).
11. If a user ID of “*” is found on the standard access list of the RACF profile protecting any type of DB2 privilege that allows access (according to the description in sections 7.3.4.1 to 7.3.4.20) provides sufficient access and the current user is defined to RACF without the RESTRICTED attribute, access is granted (AC.4-DB2-10)
12. If the universal access authority (UACC) for the resource provides sufficient access authority (see Note) and the requesting user is not defined with the RESTRICTED attribute, access is granted (AC.4-DB2-11).
13. If the universal access authority (UACC) for the RACF profile protecting any type of DB2 privilege that allows access (according to the description in sections 7.3.4.1 to 7.3.4.20) provides sufficient access and the current user is defined to RACF without the RESTRICTED attribute, access is granted (AC.4-DB2-12).
14. RACF checks the user’s access authority in the conditional access list specified with WHEN(TERMINAL), WHEN(CONSOLE), WHEN(APPCPORT), WHEN(JESINPUT) or WHEN(SERVAUTH). If the user is in the list, if the user meets the specified condition (such as logged on at the specified terminal), and if the specified access authority is sufficient to allow access, access is granted (AC.4-DB2-13).
15. RACF determines whether the user has access to the resource because the user is a member of a group that meets a condition specified on the conditional access list specified with WHEN(TERMINAL), WHEN(CONSOLE), WHEN(APPCPORT), WHEN(JESINPUT) or WHEN(SERVAUTH) (AC.4-DB2-14). Which group is used depends on whether list-of-groups processing is in effect. RACF determines which group to use according to the following rules:
    a. If list-of-groups processing is not in effect, RACF uses only the user’s current connect group (AC.4-DB2-15).

b. If list-of-groups processing is in effect, RACF finds all of the groups to which the user is connected that are also in the access list. Of these groups, RACF uses the group that has the highest access authority to the resource.

c. If the group to be used according to the preceding rules has sufficient access authority to allow the requested access (see Note), access is granted (AC.4-DB2-16).

16. If a user ID of "*" is found on the conditional access list specified with WHEN(TERMINAL), WHEN(CONSOLE), WHEN(APPCPORT), WHEN(JESINPUT) or WHEN(SERVAUTH), and if the current user is defined to RACF without the RESTRICTED attribute, and if the current user meets the specified condition (such as logged on at the specified terminal), and the access authority granted to * is sufficient to allow the requested access, access is granted (AC.4-DB2-17).
17. RACF checks the user's access authority in the conditional access list specified with WHEN(PROGRAM). If the user is in the list, if the user meets the specified condition (such as running the specified program), and if the specified access authority is sufficient to allow access, access is granted (AC.4-DB2-18).
18. If none of those conditions has granted access, access is denied (AC.4-DB2-19);

and, if access is granted by the above algorithm, the following is evaluated:

1. When a table has row access control activated and has one or more row permissions associated, then access to a table row is allowed if the row meets the WHERE search condition defined in at least one of the row permissions (AC.4-DB2-2c).
2. When a table has column access control activated and the column has a column mask associated, then access to a column value is allowed after applying the CASE expression defined in the table column (AC.4-DB2-2d).

Note 1: Sufficient access means that a user with at least **READ** authorization to the resource has sufficient access.

Note 2: Trusted contexts allow the assignment of a different primary authorization ID, a database role to the associated DB2 process, based on the definition of a trusted context. In this case, the access evaluation algorithm takes into account these security attributes (a database role is only valid in trusted contexts).

Note 3: It should be noted, that the PRIVILEGED attribute is one for a started task.

7.3.4.1 DB2 administrative authorities

Administrative authorities are defined similarly to the other privileges. They define the administrative roles for DB2. They are defined in the DSNADM class and a resource name in this class has the following structure (in a multiple subsystem scope):

DB2-subsystem.[object-name.]authority-name

The following table lists the administrative authorities and their corresponding RACF object qualifier, when it applies:

DB2 Administrative authority	RACF object qualifier
DBADM	*database-name*
DBCTRL	*database-name*
DBMAINT	*database-name*
PACKADM	*collection-ID*
SYSADM	—
SYSCTRL	—
SYSOPR	—
SECADM	—
DATAACCESS	—
ACCESSCTRL	—
SQLADM	—
SYSDBADM	—

Table 7 – DB2 administrative authorities

The following subchapters specify for each DB2 object protected by RACF, the DB2 authorities defined for the object and the RACF profile protecting the DB2 privilege for the DB2 object that the user requires sufficient access to. See the Note at the end of Section 7.3.3.2 for the definition of '*sufficient access*'.

The roles defined in DB2 and the security claims related to roles are described in more detail in chapter 7.4.3.

7.3.4.2 DB2 objects for owner ACEE authorization

There are three scenarios where owner ACEE can be used for authorization checks. Owner could be a RACF user (possibly different from the primary authid) or a RACF group.

- **Static SQL authorization**: The static SQL statement is embedded within an application program. The statement is prepared when the program is bound to DB2 and the authorization is checked during this bind process. The bind process allows the binder (primary authorization ID) to specify an owner for the package / plan. The default owner is the binder (AC.4-DB2-45a).

  BIND and REBIND PACKAGE - Package owner is checked for BINDADD/BIND privilege & CREATEIN privilege on the collection for bind process, as well as the privileges required to execute the static SQL statements in the package (AC.4-DB2-45b).

  BIND and REBIND PLAN - Plan owner is checked for BINDADD/BIND privilege for bind process. If PKLIST is specified, plan owner is checked for EXECUTE privilege on each package specified in the PKLIST (AC.4-DB2-45c).

- **Dynamic SQL authorization**: Dynamic SQL statement is prepared at run time and the authorization is checked at run time. The bind process DYNAMICRULES option allows to specify whether the runner (primary authorization ID) or package owner or routine definer to be used for dynamic SQL authorization (AC.4-DB2-45d).

  The following table shows the authorization ID used for dynamic SQL authorization based on DYNAMICRULES value:

DYNAMICRULES value	Authorization ID checked for dynamic SQL statements in a stand–alone application	Authorization ID checked for dynamic SQL statements in a stored procedure environment
BIND	Package owner	Package owner
RUN	Primary authorization ID	Primary authorization ID
DEFINEBIND	Package owner	Stored procedure owner
DEFINERUN	Primary authorization ID	Stored procedure owner
INVOKEBIND	Package owner	Primary authorization ID
INVOKERUN	Primary authorization ID	Primary authorization ID

Table 8 – Authorization IDs for dynamic SQL

- **Autobind**: This process automatically rebinds invalidated packages/plans. During autobind of packages, owner is checked for privileges required to execute the static SQL statements in the package. If PKLIST is specified for the plan, then during autobind of the plan, owner is checked for EXECUTE privilege on each package specified in the PKLIST (AC.4-DB2-45e).

To enable this function, new zparm AUTHEXIT_CHECK should be set to DB2 (AC.4-DB2-45f).

Note regarding database triggers: The required privileges of triggers and their associated trigger actions are checked on trigger creation time using the primary authorization ID of the creator, and remain effective until the package to which the trigger belongs gets invalidated. The TOE can be configured to do an automatic package invalidation when the privileges required by the trigger or package change.

7.3.4.3 Buffer pool privileges

A user has USE privilege to a buffer pool if any of the following is true:

- The user has sufficient access to the resource *DB2-subsystem.buffer-pool-name*.USE in the MDSNBP or GDSNBP class (AC.4-DB2-20)
- The user has sufficient access to DB2-subsystem.SYSCTRL in the DSNADM class (AC.4-DB2-21)
- The user has sufficient access to *DB2-subsystem*.SYSADM in the DSNADM class (AC.4-DB2-22)

7.3.4.4 Collection privileges

A user has the PACKADM administrative authority to a collection if any of the following is true:

- The user has sufficient access to the resource *DB2-subsystem.collection-ID*.PACKADM in the DSNADM class (AC.4-DB2-22a)
- The user has sufficient access to *DB2-subsystem*.SYSADM in the DSNADM class (AC.4-DB2-22b)

A user has CREATE IN privilege to a collection if any of the following is true:

- The user has sufficient access to the resource *DB2-subsystem.collection-ID*.CREATEIN in the MDSNCL or GDSNCL class (AC.4-DB2-23)
- The user has sufficient access to the resource *DB2-subsystem.collection-ID*.PACKADM in the DSNADM class (AC.4-DB2-24)
- The user has sufficient access to the resource *DB2-subsystem.* SYSDBADM in the DSNADM class (AC.4-DB2-24a)
- The user has sufficient access to *DB2-subsystem*.SYSCTRL in the DSNADM class (AC.4-DB2-25)

- The user has sufficient access to *DB2-subsystem*.SYSADM in the DSNADM class (AC.4-DB2-26)

7.3.4.5 Database privileges

DB2 supports the administrative authorities related to the management of databases. The user needs to have sufficient access to the resources. Three different authorities are defined:

- The *DB2-subsystem.database-name*.DBMAINT profile in the DSNADM class
- The *DB2-subsystem.database-name*.DBCTRL profile in the DSNADM class
- The *DB2-subsystem.database-name*.DBADM profile in the DSNADM class

In addition DB2 supports individual profiles in the MDSNDB or GDSNDB classes. A profile there has the structure *DB2-subsystem.database-name.privilege-name*

Individual privileges in the database class include:

Database Object Privileges	RACF Profile Qualifiers
CREATETAB	CREATETAB
CHANGE NAME QUALIFIER	no privilege name
CREATETS	CREATETS
DISPLAYDB	DISPLAYDB
DROP	DROP
IMAGCOPY, MERGECOPY, MODIFY, RECOVERY, QUIESCE	IMAGCOPY
RECOVERDB, REPORT	RECOVERDB
REORG	REORG
REPAIR, RUN REPAIR UTILITY	REPAIR
REPAIR DBD	no privilege name
RUN CHECK UTILITY, STATS	STATS
STARTDB	STARTDB
STOPDB	STOPDB
TERM UTILITY	no privilege name
TERM UTILITY ON DATABASE	no privilege name

Table 9 – Database object privileges

Access to a specific privilege for databases is granted when a user has sufficient access to one of the privileges in columns 2 to 7 of the following table marked with an 'X' in the row for the privilege in question (AC.4-DB2-27).

Privilege	Privilege in DB class	IMAGCOPY	DBMAINT	DBCTRL	DBADM	SQLADM	DATAACCESS	SYSDBADM	SYSCTRL	SYSADM	SYSOPR	DISPLAY
CHECK DATA UTILITY	STATS		X	X	X		X		X	X		
CREATETAB	X		X	X	X			X	X	X		

Privilege	Privilege in DB class	IMAGCOPY	DBMAINT	DBCTRL	DBADM	SQLADM	DATAACCESS	SYSDBADM	SYSCTRL	SYSADM	SYSOPR	DISPLAY
CHANGE NAME QUALIFIER:				X	X			X	X	X		
CREATETS	X		X	X	X			X	X	X		
DISPLAYDB	X		X	X	X			X	X	X	X	X
DROP	X			X	X			X	X	X		
MERGECOPY	IMAGCOPY	X	X	X	X		X		X	X		
IMAGCOPY, MODIFY RECOVERY, QUIESCE	X	X	X	X	X			X	X	X		
RECOVERDB, REPORT	X			X	X		X	X	X	X		
REORG	X			X	X		X		X	X		
REPAIR	X			X	X		X		X	X		
RUN REPAIR UTILITY	X			X	X	X	X	X	X	X		
REPAIR DBD									X	X		
RUN CHECK INDEX/LOB UTILITY	X		X	X	X			X	X	X		
STATS	X		X	X	X	X		X	X	X		
STARTDB	X		X	X	X			X	X	X		
STOPDB	X		X	X	X			X	X	X		
TERM UTILITY							X	X	X	X	X	
TERM UTILITY ON DATABASE			X	X	X		X	X	X	X	X	

Table 10 – Access to specific privileges for databases

7.3.4.6 Java archive privileges

Java archives are not part of the evaluated configuration.

7.3.4.7 Package privileges

The following specific privileges are defined that are evaluated for access checks:

- *DB2-subsystem.collection-ID*.PACKADM

The user must have one of the privileges with an 'X' in the row for the requested package privilege (AC.4-DB2-29):

Package Privilege	Package Owner	Privilege in Package class	PACKADM	SQLADM	SYSDBADM	DATAACCESS	ACCESSCTRL	SECADM	SYSCTRL	SYSADM
BIND	BINDAGENT	X	X		X				X	X
COMMENT ON	BINDAGENT		X		X				X	X
COPY	X	X	X		X				X	X
DROP			X		X				X	X
EXECUTE		X	X	SDP	SDP	X				X
All package privileges			X				X	X	SSN	SSN

Table 11 – Package privileges

SDP: only for system defined packages

7.3.4.8 Plan privileges

The user must have one of the privileges with an 'X' in the row for the requested plan privilege (AC.4-DB2-30):

Plan Privilege	Plan Owner	Privilege in Plan class	SYSDBADM	DATAACCESS	SYSCTRL	SYSADM
BIND	BINDAGENT	X	X		X	X
COMMENT ON	BINDAGENT		X		X	X
EXECUTE		X		X		X

Table 12 – Plan privileges

7.3.4.9 Role privileges

The user must have one of the privileges with an 'X' in the row for the requested role privilege (AC.4-DB2-40):

Role Privilege	Role Owner	Privilege in Role class	SYSCTRL	SYSADM	SECADM
COMMENT ON	X		SSN	SSN	X
CREATE ROLE			SSN	SSN	X
DROP ROLE	X		SSN	SSN	X

Table 13 – Role privileges

SSN: Only when SEPARATE_SECURITY parameter = “No”

7.3.4.10 Schema privileges

The user must have one of the privileges with an 'X' in the row for the requested schema privilege (AC.4-DB2-31):

Schema Privilege	User name matches schema name	Schema Owner	Privilege in Schema class	SYSCTRL	SYSADM	SYSDBADM
ALTERIN	X	X	X	X	X	X
CHANGE NAME QUALIFIER				X	X	X
COMMENT ON	X	X	ALTERIN	X	X	X
CREATEIN	X		X	X	X	X
DROPIN	X	X	X	X	X	X

Table 14 – Schema privileges

7.3.4.11 Sequence privileges

The user must have one of the privileges with an ‘X’ in the row for the requested sequence privilege (AC.4-DB2-41):

Sequence Privilege	User name matches schema name	Sequence Owner	Privilege in sequence class	Privilege in schema class	SYSCTRL	SYSADM	SYSDBADM	DATAACCESS
ALTER	X	X	X	ALTERIN	X	X	X	
COMMENT ON	X	X	X	ALTERIN	X	X	X	
USAGE		X	X	X		X		X

Table 15 – Sequence privileges

7.3.4.12 Storage group privileges

The user must have one of the privileges with an ‘X’ in the row for the requested storage group privilege (AC.4-DB2-32):

Storage Group Privilege	Storage Group Owner	Privilege in storage group class	SYSCTRL	SYSADM
DROP, ALTER	X		X	X
USE		X	X	X

Table 16 – Storage group privileges

7.3.4.13 Stored procedure privileges

The user must have one of the privileges with an 'X' in the row for the requested stored procedure privilege (AC.4-DB2-33):

Stored Procedure Privilege	User name matches schema name	Stored Procedure Owner	Privilege in Stored Procedure class	SYSOPR	SYSCTRL	SYSADM	SYSDBADM	SQLADM	DATAACCESS
DISPLAY	X	X	X	X	X	X	X		
EXECUTE		X	X			X	SDP	SDP	X
START	X	X		X	X	X	X		
STOP	X	X		X	X	X	X		

Table 17 – Stored procedure privileges

SDP: only for System Defined Packages

7.3.4.14 DB2 system privileges

DB2 specific privileges are defined in the MDSNSM or GDSNSM class and a resource has the form of *DB2-subsystem.privilege-name*

The user must have one of the privileges with an 'X' in the row for the requested privilege (AC.4-DB2-34):

Specific DB2 Privilege	Privilege in DB2 Specific class	SYSOPR	SYSCTRL	SYSADM	SYSDBADM	SECADM	SQLADM	DATAACCESS	DBCTRL	DBADM
ALTER BUFFERPOOL		X	X	X						
BINDADD	X		X	X	X					
BINDAGENT	X		X	X	X					
CANCEL DDF THREAD, START | STOP DDF		X	X	X						
START | STOP RLIMIT		X	X	X						
DISPLAY RLIMIT		X	X	X	X					
CREATEALIAS	X		X	X	X				X	X
CREATEDBA	CREATEDBA CREATEDBC		X	X	X					
CREATESG	X		X	X						
CREATETMTAB	CREATETMTAB CREATETAB		X	X	X					
CREATE SECURE OBJECT	X			SSN		X				
DEBUGSESSION	X			X				X		
DISPLAY, DISPLAY BUFFERPOOL	DISPLAY	X	X	X	X					
DISPLAY ARCHIVE	DISPLAY	X	X	X	X					

Specific DB2 Privilege	Privilege in DB2 Specific class	SYSOPR	SYSCTRL	SYSADM	SYSDBADM	SECADM	SQLADM	DATAACCESS	DBCTRL	DBADM
	ARCHIVE									
DISPLAY PROFILE		X	X	X	X		X			
EXPLAIN	X			X	X		X			
MONITOR1	MONITOR1 MONITOR2		X	X	X		X			
MONITOR2	X		X	X	X		X			
QUERY TUNING		X	X	X	X		X			
RECOVER BSDS	X		X	X						
RECOVER INDOUBT	X	X	X	X	X					
SET ARCHIVE	ARCHIVE	X	X	X						
START PROFILE		X	X	X	X		X			
STOP PROFILE		X	X	X	X		X			
STOPALL	X	X	X	X						
STOSPACE UTILITY	STOSPACE		X	X						
TRACE	X	X	X	X	X	X	X			
USE ARCHIVE LOG	ARCHIVE		X	X						

Table 18 – DB2 system privileges

7.3.4.15 Table privileges

The user must have one of the privileges with an 'X' in the row for the requested privilege (AC.4-DB2-35):

Table privilege	Owner of table	Privilege in Table class	DBADM	DBCTRL	DBMAINT	SYSDBADM	SQLADM	DATAACCESS	ACCESSCTRL	SECADM	SYSCTRL	SYSADM
ALTER	X	X	X			X					X	X
ALTER INDEX, DROP INDEX	ALTER		X			X					X	X
CHANGE NAME QUALIFIER			X	X		X					X	X
COMMENT ON, COMMENT ON INDEX, DROP	X		X			X					X	X
CREATE SYNONYM	No authorization checks											

Table privilege	Owner of table	Privilege in Table class	DBADM	DBCTRL	DBMAINT	SYSDBADM	SQLADM	DATAACCESS	ACCESSCTRL	SECADM	SYSCTRL	SYSADM
CREATE VIEW		SELECT	T			SCT					SCT	X
DELETE	X	X	X			SCT APE	SCT APE	APE	SCT APE	SCT	SCT APE	APE(SSN)
DROP ALIAS	X					X					X	X
DROP SYNONYM	No authorization checks											
INDEX	X	X	X			X					X	X
INSERT	X	X	X			SCT APE	SCT APE	APE	SCT APE	X	SCT APE	APE(SSN)
LOAD	X	X	X	X				X			X	X
LOCK TABLE	X	SELECT	X					X			X	X
REFERENCES	X	REFERENCES ALTER REFERENCES (column qualifier)	X			X					X	X
REFRESH	Not supported in CC evaluation											
RENAME INDEX	X		X	X	X	X					X	X
RENAME TABLE	X		X	X	X	X					X	X
SELECT	X	X	X			SCT	SCT	X	SCT	SCT	SCT	X
TRIGGER	X	TRIGGER ALTER	X			X					X	X
UNLOAD	X	UNLOAD	X			SCT	SCT	X	SCT	SCT	SCT	X
UPDATE	X	UPDATE UPDATE (column qualifier)	X			SCT APE	SCT APE	APE	SCT APE	SCT	SCT APE	APE(SSN)
“Any table” privilege	X	DFP				X	X	X	SCT	SCT	SCT	X

Table 19 - Table privileges

T: only tables (not views)

SCT: only for system catalog tables

SSN: only when SEPARATE_SECURITY parameter = “No”

APE: SYSIBM.SYSAUDITPOLICIES table excluded

DFP (derived from other privileges): The “Any Table” privilege (used by the DESCRIBE TABLE SQL statement) is granted if any of the following privileges is granted on the object: SELECT, INSERT, UPDATE, DELETE, REFERENCES, ALTER or INDEX.

7.3.4.16 Tablespace privileges

The user must have one of the privileges with an 'X' in the row for the requested tablespace privilege (AC.4-DB2-36 and AC.4-DB2-37):

Tablespace privilege	Owner of table	Privilege in Table class	DBADM	SYSDBADM	SYSCTRL	SYSADM
DROP, ALTER			X	X	X	X
USE		X	X	X	X	X

Table 20 – Tablespace privileges

7.3.4.17 Trusted context privileges

The user must have one of the privileges with an 'X' in the row for the requested trusted context privilege (AC.4-DB2-42):

Trusted Context Privilege	Trusted Context Owner	Privilege in Trusted Context class	SYSCTRL	SYSADM	SECADM
ALTER TRUSTED CONTEXT				SSN	X
COMMENT ON TRUSTED CONTEXT	X		SSN	SSN	X
CREATE TRUSTED CONTEXT				SSN	X
DROP TRUSTED CONTEXT	X		SSN	SSN	X

Table 21 – Trusted context privileges

SSN: Only when SEPARATE_SECURITY parameter = ”No”

7.3.4.18 View privileges

The user must have one of the privileges with an 'X' in the row for the requested privilege (AC.4-DB2-38):

Specific view privilege	Owner of view	Privilege in view class	DBADM	SYSCTRL	SYSADM	SYSDBADM	SQLADM	DATAACCESS	ACCESSCTRL	SECADM
ALTER	X			X	X	X				
COMMENT ON	X			X	X	X				

DELETE (for updatable views)	X	X	X		X	SCT APE	SCT APE	APE	SCT APE	SCT
DELETE (for read-only views)		X			X			X		
DROP	X			X	X	X				
INSERT (for updatable views)	X	X	X		X	SCT APE	SCT APE	APE	SCT APE	SCT
INSERT (for read-only views)		X			X			X		
INSTEAD OF TRIGGER	X			X	X	X				
REGENERATE VIEW	X			X	X	X				
SELECT		X			X			X		
UPDATE (for updatable views)	X	X	X		X	SCT APE	SCT APE	APE	SCT APE	SCT

UPDATE (for read-only views)		UPDATE
		UPDATE (column qualifier)
					X			X		

“Any table” privilege		DFP		SCT	X	X	X	X	SCT	SCT

Table 22 – View privileges

SCT: only System Catalog Tables

APE: SYSIBM.SYSAUDITPOLICIES table excluded

DFP (derived from other privileges): The “Any Table” privilege (used by the DESCRIBE TABLE SQL statement) is granted if any of the following privileges is granted on the object: SELECT, INSERT, UPDATE or DELETE.

7.3.4.19 Global variable privileges

The user must have one of the privileges with an ‘X’ in the row for the requested global variable privilege (AC.4-DB2-43):

Global Variable Privilege	Global Variable Owner	Privilege in Global Variable class	DATAACCESS	SYSADM
READAUT	X	X	X	X
WRITEAUT	X	X	X	X

Table 23 – Global variable privileges

7.3.4.20 Trigger Privileges

The user must have one of the privileges with an 'X' in the row for the requested trigger privilege (AC.4-DB2-44):

Trigger Privilege	Trigger Owner	Privilege in Trigger class	DATAACCESS	SYSADM
CHANGE OWNER	X		X	X

Table 24 – Trigger Privileges

7.3.5 Row and Column access control

Row and Column access control adds a finer level of granularity to the Discretionary Access Control Policy.

A row permission is a database object that expresses an access control rule for a row of a specific table. A row permission is in the form of a search condition that describes to which rows users have access. Row permissions are applied after table privileges (like SELECT or INSERT) are checked. Multiple row permissions can be created for a table.

When an ALTER TABLE statement is used to explicitly activate row access control for a table, a default row permission is implicitly created for the table which prevents all access to the table. After row access controls have been activated for a table, if the table is referenced explicitly in a data change statement and if multiple row permissions are defined for the table, a row access control search condition is derived by using the logical OR operator with the search condition of each defined row permission (AC.4-DB2-47).

A column mask is a database object that expresses an access control rule for a specific column in a table. A column mask is in the form of a CASE expression that describes to which column values users have access. Column masks are applied after table privileges (like SELECT or INSERT) are checked.

Multiple column masks can be created for a table, but only one column mask can be created for each column in a table (AC.4-DB2-48).

A row permission or a column mask can be created before row or column access control is enforced for a table. The definition of the row permission and the column mask is stored in the DB2 catalog. However, the permission and the mask do not take effect until they are activated (ACTIVATE ROW ACCESS CONTROL and ACTIVATE COLUMN ACCESS CONTROL clauses in the ALTER TABLE statement) (AC.4-DB2-49).

The search condition of a row permission and the case expression of a column mask can contain the following functions that allows enforcing access control based on the user's attributes:

- SESSION_USER: the primary authorization ID.
- VERIFY_GROUP_FOR_USER: verifies whether the group authorization ID of the primary authorization ID matches the given value. In the evaluated configuration, this has the same effect as SESSION_USER (RACF returns the primary authorization ID as the group authorization ID).
- VERIFY_ROLE_FOR_USER: verifies whether the role of the primary authorization ID matches the given value.
- VERIFY_TRUSTED_CONTEXT_FOR_USER: verifies whether the role acquired in a trusted context and matches the given value.

7.3.5.1 Row permissions

There are no explicit privileges for this DB2 object: the user must have the SECADM administration authority to create or alter permissions (AC.4-DB2-50).

7.3.5.2 Column masks

There are no explicit privileges for this DB2 object: the user must have the SECADM administration authority to create or alter column masks (AC.4-DB2-46).

7.3.6 DB2 internal access checking

In the evaluated configuration access checking is configured to be performed by RACF. To avoid a "mix" of access checking by RACF and access checking by DB2, a set of generic profiles defined in the “DB2 Common Criteria Guide” has to be defined with UACC(NONE) to avoid that RACF returns with a "resource not defined" return code resulting in DB2 using both RACF and DB2 internal access checking for checking access to one resource. This would otherwise lead to inconsistent states of the access control model. Further, the RACF access control module has error option &ERROROPT set to 2, which causes DB2 to shut down if the RACF module fails to initialize, abends or returns an unexpected return code. This ensures that authorization is not switched to DB2 internal access checking should RACF malfunction.

7.4 Security management

7.4.1 Security management in RACF

7.4.1.1 User and Group Management

To create a TOE user, a user profile for the new user has to be created in RACF. Each user profile consists of a base segment and optional segments for the use of specific subsystems. RACF also supports a special user profile segment, CSDATA, for which the security administrator can specify the format and content of the data fields using other profiles in the CFIELD class, as well as specifying access rules in the FIELD class to determine which users can view or update data in the segment.

To create or modify a user profile, a user must have one of the following authorities:

- the SPECIAL role as a general system administrator;
- the UPDATE authority to the fields in a non-base segment of the profile he wants to modify through field-level access checking;
- to create a new user: is connected to a group that has the group-SPECIAL role and has the CLAUTH attribute for the USER class and is the owner of or has JOIN authority in the new user’s default group. Note that the following roles of the ADDUSER command can not be assigned in this case: OPERATIONS, SPECIAL, and AUDITOR;
- to modify the attribute of a user: the CLAUTH attribute for the user class. Note that only the CLAUTH and NOCLAUTH attribute can be changed.

RACF allows groups of users to be defined, making the management of users and user attributes and roles easier. To create a new group, a group profile must be defined in RACF. A group profile (as a user profile) consists of a base segment and (optional) other segments. As with the user profiles all group attributes related to the security policy as defined in this Security Target are contained in the base segment of the group profile. Each group defined in RACF must be owned by a RACF-defined user or by its superior group. Ownership of a group is assigned with the ADDGROUP command when a new group profile is created and can be changed with the ALTGROUP command used to change an existing group profile.

Management of TOE user and group profiles occurs primarily via the RACF commands described later (ADDUSER, ALTUSER, DELUSER, LISTUSER, ADDGROUP, ALTGROUP, DELGROUP, LISTGRP). Administrators enter these commands while running in a TSO session.

The base segment of a user profile within RACF contains (among other data not relevant for the security functions defined in this Security Target) the following:

Name	Description
USERID	User’s identification (a maximum of 8 characters).
NAME	User’s name (not security relevant, because the user is allowed to change his name).
OWNER	Owner of the user’s profile.
DFLTGRP	User’s default group. (Note: A user may specify, at login time, any group he or she is connected to as the current default group. This does not change the DFLTGRP value in the profile.)
AUTHORITY	User’s authority in the default group (use, create, connect, join).
PASSWORD	User’s password. The user ID is DES-encrypted using the password (padded with blanks) as a key. Users who have no password and no password phrase are said to have the PROTECTED attribute, and can not logon to the system via any mechanism that uses a password, password phrase, or PassTicket.
PHRASE	Optional password phrase. Users who have a phrase must also have a password.
REVOKE	This attribute consists of a flag and a date. The date parameter specifies the date on which the user is revoked. The flag indicates that the user is revoked. The user is revoked, if either the flag is set or the actual date is after the revoke date, if defined.
RESUME	Date on which RACF lets the user have access to the system again.
UACC	Default universal access authority for resource profiles that the user defines. Only applicable to DATASET and a few general resource classes).
WHEN	Days of the week and hours of the day during which the user has access to the system.
CLAUTH	Classes in which the user can define profiles.
SPECIAL	Gives the user the system-wide SPECIAL attribute.
AUDITOR	Gives the user the system-wide AUDITOR attribute.
OPERATIONS	Gives the user the system-wide OPERATIONS attribute.
TRUSTED	Gives the user the system-wide TRUSTED attribute.
RESTRICTED	Gives the user the system-wide RESTRICTED attribute.
MODEL	Name of the data set model profile to be used when creating new data set profiles, either generic or discrete.
SECLABEL	User’s default security label (evaluated in Labeled Security Mode only).
CERTNAME	The names of the profiles in the DIGTCERT (digital certificate) class that are related this RACF user ID.
CERTLABL	The certificate labels associated with the profiles in the DIGTCERT class that are related to this RACF user ID.

Table 25** – **User Profile

User roles and attributes are extraordinary capabilities, restrictions, or environments that can be assigned to a user, either all of the time or when the user is connected to a specific group or groups. User attributes are stored and managed within the RACF database.

When a role or attribute is to apply only to a specific group or groups, it is specified at the group level and is called a group-related user attribute. For example, user attributes that are specified in an ADDUSER or ALTUSER command are stored in the user’s profile and are in effect regardless of the group to which the user is connected.

RACF maintains the roles and attributes specified in this section in fields in the user profile.

A user who has the SPECIAL attribute at the system level can issue all RACF commands (but not all operands. There are AUDITOR-only operands related to the configuration of the audit function that only a user with the AUDITOR attribute is allowed to use). The SPECIAL attribute gives the user full control over all of the RACF profiles in the RACF database. The SPECIAL attribute can also be assigned at the group level. Such a user with the group-SPECIAL attribute has full control over all of the profiles within the scope of the group.

A user with the SPECIAL role in his user profile is regarded as a system administrator. He can:

- add, delete, list and modify user, group, DATASET and other profiles
- list and define RACF general options (except options related to auditing)

A system administrator can delegate administrative activities to users such that they can administer profiles belonging to a defined group. He does this by assigning such users the group-SPECIAL attribute. Those users then have administrative capabilities within the group they were assigned the group SPECIAL attribute. Users with the attribute group-SPECIAL cannot use general RACF options of the SETROPTS command (except for the REFRESH GENERIC and LIST operands).

The AUDITOR attribute is given only to users who are responsible for auditing RACF security controls and functions. To provide a check and balance on RACF security measures, the AUDITOR attribute should be given to security or group administrators other than those who have the SPECIAL attribute. The AUDITOR attribute can also be assigned at the group level. Such a user with the group-AUDITOR attribute can control the audit configuration within the scope of the group where the attribute was assigned

A user with the AUDITOR attribute can define and modify the audit related options in user and the auditor related options for resource profiles. This allows him to define which activities are to be recorded in the audit trail. He can also list the content of any profile and set the system wide audit related options using the SETROPTS command. Those options are:

- AUDIT or NOAUDIT (for each profile class)
- CMDVIOL or NOCMDVIOL
- LOGOPTIONS (for each profile class)
- OPERAUDIT or NOOPERAUDIT
- SAUDIT or NOSAUDIT
- SECLABELAUDIT or NOSECLABELAUDIT

Audit configuration can also be delegated at the group level by giving the group-AUDITOR attribute to a user.

A started task (acting on behalf of a user) can be assigned the PRIVILEGED attribute.

Revocation of the RACF user ID associated with a user: As all user authentication occurs via RACF, and all users have a RACF identity, the administrator can revoke a user by using the ALTUSER command with the REVOKE operand. Note that this will not cover immediate revocation, but it will prevent the user from entering the system in the future.

7.4.1.2 Resource Management

RACF makes access decisions based on information stored in profiles or in the metadata associated with z/OS UNIX objects. RACF manages the following resource profiles:

- Data set profiles
- General resource profiles

General resource profiles apply to a number of resources defined as protected resources in this Security Target. The structure of the profiles in RACF used to protect those resources is identical, but the semantics of specific access rights is defined by the manager of the resource and may therefore differ depending on the type of resource.

Profiles consist of a base segment and optionally a set of non-base segments. Fields within non-base segments can be individually protected using the field-level access control possibilities provided by RACF.

Field-level access control allows the control of READ and UPDATE access to individual fields within a segment other than the base segment of a RACF profile. This access is based on RACF profiles in the FIELD class. Profiles in this class have the structure of *profile-type.segment-name.field-name* where *profile-type* is either the class name of a general resource profile or one of DATASET, GROUP, or USER.

Different profile classes/types can have different segments and the name of the segment that contains the field for which access is controlled is specified as the second part of the profile. Different segments have different fields identified by their name and the name of the field is the third part of the profile controlling access to the field. The access control algorithm for access to general resources is used also for the FIELD class.

Fields in segments are related to operands of RACF commands or the R_admin callable service used to manage profiles and the purpose of field level access control is to provide a mechanism that allows the definition of fine-grained access control to use those command operands or list the content of individual fields

In order to use field-level access control, the FIELD class needs to be active and SETROPTS RACLIST needs to be activated for the FIELD class. Otherwise only a user with the SPECIAL or AUDITOR attribute has access to fields.

When the FIELD class is active and SETROPTS RACLIST is activated for the FIELD class, users with the SPECIAL or AUDITOR attribute can list all fields regardless of the access definition in the profile protecting access to the field.

To allow users to read or update fields in their own user profile protected by field-level access control a userid of &RACUID can be specified in the PERMIT command for the profiles in the FIELD class related to the fields in profiles of type USER. This does not allow this user access to those fields in the user profiles of other users.

Other protected resources are protected by general resource profiles that contains the resource class and the resource attributes. An access control list with entries defining the access types for individual users and / or groups can be defined for each such resource profile. The semantics of the individual access rights are defined by the resource manager responsible for the management of the resources protected by such a profile. Different resource classes may have different resource managers responsible for the protection and management of the resources within the class.

The structure of a general resource profile is defined in the following table (omitting fields that are not relevant for the Security Policy):

Name	Description
Class name	Name of the resource class the profile belongs to
Profile name	Name of the generic resource profile
OWNER (user ID or groupname)	The owner of the profile. Note that being the owner of a resource profile does not, by itself, allow a user to have access to the resource or resources that are protected by the profile – this is a different ownership concept than the one described in section 7.3.3.2.
NOTIFY	The user who is to be notified whenever RACF uses this profile to deny access to a resource
UACC	The universal access authority for the resource or resources protected by the profile
AUDIT	The type of auditing to be performed for the resource or resources protected by the profile
FROM	The name of a profile that is to be used as a model
FCLASS	The class of the model profile
FGENERIC	A setting that indicates that the model profile name is to be treated as a generic name
FVOLUME	The volume that is to be used to locate the model profile
CATEGORY	The security categories to be assigned to the resource or resources protected by the profile (evaluated in Labeled Security Mode only)
SECLABEL	The security label of the resource or resources protected by the profile (evaluated in Labeled Security Mode only)
SECLEVEL	The security level of the resource or resources protected by the profile (evaluated in Labeled Security Mode only)
LEVEL	An installation-defined level
SINGLEDSN	The tape volume protected by this profile can contain only one data set (TAPEVOL class only)
TIMEZONE	The time zone in which a terminal resides (TERMINAL class only)
TVTOC	A setting that specifies that RACF is to create a tape volume table of contents (TVTOC) when a user creates the first output data set on the tape volume (TAPEVOL class only)
WHEN	The times when the terminal or terminals protected by the profile can be used to access the system (TERMINAL class only)

Table 26** – **Resource Profile Structure

7.4.1.3 RACF configuration and management

The SPECIAL role can define system wide-options of RACF with the SETROPTS command:

- Choose the resource classes that RACF is to protect.
- Set the universal access authority (UACC) for otherwise undefined terminals.
- Specify logging of certain RACF commands and events.
- Enable or disable list-of-groups access checking.
- Display options currently in effect.
- Enable generic profile checking for all active classes
- Control global access checking for selected individual resources or generic names with selected generalized access rules

- Initiate refreshing of in-storage generic profile lists and global access checking tables.
- Enable or disable shared profiles through RACLIST processing for general resources.
- Activate auditing of access attempts to RACF-protected resources based on installation-defined security levels.
- Activate enhanced generic naming
- Control whether a profile creator's user ID is automatically added to the profile's access list.

Addtionally, the following options can be configured:

- Establish password syntax rules.
- Activate password processing for checking previous passwords, limit invalid password attempts, and warn of password expiration.
- Set the passwords for authorizing use of the RVARY command.
- Activate profile modeling for GDG, group, and user data sets.
- Activate protection for data sets with single-level names.
- Control logging of real data set names.
- Control the job entry subsystem (JES) options implemented in RACF.
- Activate tape data set protection.
- Enable protection of data sets by default (PROTECTALL(FAILURES)).
- Enable the erasure of scratched DASD data sets.
- Activate program control.

7.4.2 Security management of DB2

Users of DB2 need to be defined in RACF and the management of users is performed by RACF as described in the section "User and group management" above.

Security Management of DB2 is split into several aspects:

1. Management of RACF-controlled access rights to DB2 objects
2. Management of the DB2 audit trail
3. Management of database roles and trusted contexts
4. Management of row and column access control

RACF controlled access rights are managed using the RACF commands described in [ZOSST] section 8.4.6. Those commands are used to create and modify profiles in the RACF classes for DB2 objects as well as the PERMIT command used to manage access rights for those profiles (SM.3-DB2-1).

Management of the DB2 audit trail is performed by DB2 commands (starting and stopping the audit trace using the START TRACE and STOP TRACE DB2 commands) (SM.3-DB2-2) and by SQL commands (setting or modifying the audit attribute of tables) (SM.3-DB2-3). Starting and stopping the DB2 audit trail is restricted to users with SQLADM, SYSDBADM, SECADM, SYSOPR, SYSCTRL or SYSADM authority or users with the TRACE privilege (SM.3-DB2-4). Setting or modifying the audit attribute of a table requires either SYSDBADM, SYSADM or SYSCTRL authority, DBADM authority for the database the table is part of, ownership of the table or ALTER privilege on the table (SM.3-DB2-5).

Database roles and trusted contexts are DB2 objects managed using the CREATE, ALTER and DROP SQL commands (SM.3-DB2-8). Control access to users on these objects and their management operations is performed by RACF as the rest of the DB2 objects.

Row permissions are DB2 objects managed using the CREATE PERMISSION, ALTER PERMISSION and DROP SQL commands (SM.3-DB2-9); row access control can also be activated or deactivated with the ACTIVATE, DEACTIVATE ROW ACCESS CONTROL clause of the ALTER TABLE statement (SM.3-DB2-10). Control access to users on these objects and their management operations is performed by RACF as the rest of the DB2 objects.

Column masks are DB2 objects managed using the CREATE MASK, ALTER MASK and DROP SQL commands (SM.3-DB2-11); column access control can also be activated or deactivated with the ACTIVATE, DEACTIVATE COLUMN ACCESS CONTROL clause of the ALTER TABLE statement (SM.3-

DB2-12). Control access to users on these objects and their management operations is performed by RACF as the rest of the DB2 objects.

7.4.3 DB2 user attributes and user roles and database roles

DB2 supports the following user roles, known in DB2 as administrative authorities:

- SYSADM
- SYSCTRL
- SYSOPR
- SECADM
- System DBADM or SYSDBADM
- DATAACCESS
- ACCESSCTRL
- Install SYSADM
- Install SYSOPR
- DBADM
- DBCTRL
- DBMAINT
- SQLADM
- PACKADM

SYSADM, SYSCTRL and SYSOPR are user roles with privileges on the DB2 subsystem level.

SECADM, SYSDBADM, DATAACCESS, ACCESSCTRL and SQLADM are also user roles with privileges on a DB2 subsystem. These administrative authorities allow the separation of duties between structure and data management. When the SEPARATE_SECURITY parameter is set to yes, the SYSADM and SYSCTRL roles have less privileges.

DBADM, DBCTRL and DBMAINT are user roles with privileges on the database level within a defined DB2 subsystem.

PACKADM is a user role defined on the level of a collection.

Install SYSADM and Install SYSOPR are user roles used for the initial setup and configuration of DB2. They should be disabled after the initial configuration.

User roles are defined by dedicated profiles in the DSNADM class (SM.3-DB2-6). A user gets a user role assigned when he is assigned sufficient access (please refer to section 7.3.3.2 for a definition of ‘*sufficient access*’) to the profile associated with the user role (SM.3-DB2-7). This can be done by any user that is allowed to assign permission to those profiles according to the rules implemented in RACF. The privileges associated with each role are defined in the description of the discretionary access rights in this ST.

7.4.4 Trusted contexts and database roles

Trusted contexts allow the assignment of a different primary authorization ID, a database role, to the associated DB2 process, based on the definition of a trusted context. In this case, the access evaluation algorithm takes into account these new security attributes. Database role is only valid in trusted contexts (SM.DB2-V12-TC).

7.4.5 Transfer of Database Object Ownership

By means of the TRANSFER OWNERSHIP SQL command, the TOE enables the object owner and administrators with the SECADM authority transfer the ownership of a database or system object to another user (SM.DB2-V12-TO).

7.5 Auditing

The generation of audit records, protection of the audit trail and audit configuration and management functionality is provided by the z/OS platform and described in the accordant chapters of [ZOSST].

7.5.1 Generation of audit records

The TOE provides a general facility to collect data required for auditing and accounting services, which the TOE forwards to a component of z/OS for recording. This component of the TOE environment, the System Management Facilities (SMF), collects and records system and job-related information that an installation can use for such tasks as the following:

- Billing users
- Reporting reliability
- Analyzing the configuration
- Scheduling jobs
- Summarizing direct access volume activity
- Evaluating data set activity
- Profiling system resource use
- Maintaining system security

This component is used by the TOE to store and manage the security-related auditing information the TOE has generated as required by FAU_GEN.1 and FAU_GEN.2.

Each SMF record consists of a standard header which contains (among other information) the type of the record and the time the record was produced. The standard header is produced by the calls to the SMFWTM or SMFEWTM services. Especially the time and date are filled in by SMF and not by the caller.

One record type is usually reserved for a whole class of events where the individual events are identified by the record subtype or event code in the header of the SMF record.

RACF as the central access control function has three SMF record types reserved for its use (80, 81, 83), with record type number 80 being the most important one. The information recorded in this record type contains (among other non security related information):

- The record type
- Time stamp (time and date) (filled in by the SMF component of z/OS)
- System identification
- Event code and qualifier
- User identification
- Group name
- Authorities used to successfully execute commands or access resources
- Reasons for logging
- Command processing error flag
- Foreground user terminal ID or other port-of-entry information

- Job log number (job name, entry time, and date)
- RACF version, release, and modification number
- SECLABEL of user (relevant in Labeled Security Mode only)

Each record contains further data specific to the event code and qualifier

z/OS provides the capability to search the audit trail for specific events and relate them such that events related to a specific user.

Tools exist that allow user with access to the audit trail data to search the audit trail for specific events, for audit events related to specific jobs / users and other criteria. Tools exist that transfer the audit data into human readable format.

7.5.2 Event Notifications generated by RACF

RACF can send an ENF type 62 signal to listeners when a SETROPTS RACLIST command affects in-storage profiles used for authorization checking. RACF sends a signal when a SETROPTS RACLIST, SETROPTS NORACLIST, or SETROPTS RACLIST REFRESH command is issued for a class, activating, deactivating, or updating the profiles. Signals are sent for a class in the static class descriptor table if SIGNAL=YES was specified on the ICHERCDE macro that defined the class. Signals are sent for a class in the dynamic class descriptor table if SIGNAL(YES) was specified on the CDTINFO keyword of the RDEFINE or RALTER command that defined the class.

7.5.3 Audit configuration and management

Within the system configuration it needs to be decided, which SMF records shall be generated by z/OS. Three record types (type 80, 81, and 83) are dedicated to RACF. Which events are actually recorded with those records can be configured by a user with the AUDITOR attribute in his RACF user profile. In addition record type 30 is generated for a number of security related events.

Because a set of mandatory events is always audited, not all audit records (such as unauthorized attempts to access the system or changes to the status of the RACF database) can be configured.

In addition, resource profiles can define which events related to this resource are audited. The owner of a resource profile as well as a user in the AUDITOR role are able to change the entries related to auditing within the resource profile.

Individual users can be audited by using UAUDIT/NOUAUDIT parameter on the ALTUSER command. This user’s actions are then subject to audit.

The system can be configured to send certain audit messages to the security console to immediately alert operators of detected policy violations.

RACF uses the interfaces defined by the SMF component of z/OS to have SMF finalize and store the audit records. SMF adds a standard header to the audit record, which contains the time and date the record was produced.

The RACF SMF data unload utility (IRRADU00) can be used to create a sequential file from the security relevant audit events stored in the SMF audit trail. The resulting sequential file can either be viewed directly or used for further processing like with the utility DFSORT (which is part of the TOE environment), which can be used to create reports by selecting specific records and further structure the reports.

7.5.4 Auditing in DB2

Audit records related to access control checking for DB2 objects are also generated by RACF in the same way as audit records related to access control checking of other objects protected by RACF. Defining what is audited is done by the AUDIT parameter of the RDEFINE and RALTER command or the GLOBALAUDIT parameter of the RALTER command (AU.3-DB2-1).

In the case of access control functions performed for DB2 objects RACF will generate SMF records as for any other object and the DB2 trace records will hold additional information about attempted and actual access to DB2 objects. In the evaluated configuration DB2 audit trace records will also be stored using SMF and the protection functions of SMF to protect the audit trail also apply for the DB2 audit trace records (AU.3-DB2-2).

DB2 generates SMF record type 102 for security relevant audit data using the DB2 trace facility. DB2 provides the START TRACE command to start the generation of audit trace records and the STOP TRACE command to stop generation of DB2-related audit records (AU.3-DB2-3).

Among other things, the audit trace records can indicate the following information (AU.3-DB2-4):

- The ID that initiated the activity
- The LOCATION of the ID that initiated the activity (if the access was initiated from a remote location)
- The type of activity and the time that the activity occurred
- The DB2 objects that were affected
- Whether access was denied
- The owner of a particular plan and package
- The database alias (DBALIAS) that was used to access a remote location or a location alias that was accepted from a remote application

DB2 defines a set of audit classes that characterize the type of events traced. The following table provides a short description of the audit classes and the events that are traced for each class:

Audit class	Audit events that are traced
1	Access attempts that DB2 denies because of inadequate authorization (AU.3-DB2-5). This class is the default.
2	Explicit GRANT and REVOKE statements and their results. This class does not trace implicit grants and revokes. Note that GRANT and REVOKE have no effect in the evaluated configuration and therefore those events are not security relevant. **Note that this has no meaning in the evaluated configuration.**
3	Traces CREATE, ALTER, and DROP operations against an audited tables or a table that is enabled with with row-level granularity. For example, it traces the deletion of a table as the result of a DROP TABLESPACE or DROP DATABASE; it also traces the updates to a table created with the AUDIT CHANGES or AUDIT ALL clause (AU.3-DB2-6).
4	Changes to audited tables. Only the first attempt to change a table, within a unit of recovery, is recorded. (If the agent or the transaction issues more than one COMMIT statement, the number of audit records increases accordingly.) The changed data is not recorded, only the attempt to make a change is recorded. If the change is not successful and is rolled back, the audit record remains; it is not deleted. This class includes access by the LOAD utility. Accesses to a dependent table that are caused by attempted deletions from a parent table are also audited. The audit record is written even if the delete rule is RESTRICT, which prevents the deletion from the parent table. The audit record is also written when the rule is CASCADE or SET NULL, which can result in deletions that cascade to the dependent table (AU.3-DB2-7).
5	All read accesses to tables that are identified with the AUDIT ALL clause. As in class 4, only the first access within a DB2 unit of recovery is recorded. References to a parent table are also audited (AU.3-DB2-8).

Audit class	Audit events that are traced
6	The bind of static and dynamic SQL statements of the following types: • INSERT, UPDATE, DELETE, CREATE VIEW, and LOCK TABLE statements for audited tables. Except for the values of host variables, the audit record contains the entire SQL statement (AU.3-DB2-9). • SELECT statements on tables that are identified with the AUDIT ALL clause. Except for the values of host variables, the audit record contains the entire SQL statement (with record type IFCID 0350 included) (AU.3-DB2-10).
7	Assignment or change of an authorization ID because of the following reasons (AU.3-DB2-11): • Changes through a default or user-written exit routine (not relevant for the evaluated configuration). • Changes through a SET CURRENT SQLID statement • An outbound or inbound authorization ID translation (inbound translation is not relevant for the evaluated configuration) • An ID that is being mapped to a RACF ID from a Kerberos security ticket (not relevant for the evaluated configuration)
8	The start of a utility job, and the end of each phase of the utility.
9	Various types of records that are written to IFCID 0146 by the IFI WRITE function.
10	CREATE and ALTER TRUSTED CONTEXT statements, establish trusted context information and switch user information
11	Audit the use of any administrative authority and the successful execution of any authorization ID.

Table 27 – Audit classes

In addition the AUDIT clause in the CREATE TABLE or ALTER TABLE command can be used to audit access to specific tables (AU.3-DB2-12). All tables with row level security are automatically treated as if the AUDIT ALL clause is set for the table (AU.3-DB2-13).

Auditing can be started for a particular plan name, a defined set of plans, a particular primary authorization ID, a defined set of IDs, defined classes of auditing with individual audit trace record types (IFCIDs) specified (AU.3-DB2-14).

Auditing can also be started for a defined set of audit policies (AU.3-DB2-14a).

An audit policy is a set of criteria that determines the categories to be audited. It helps configuring and controlling the audit requirements of the security policies and to monitor data access by applications and individual users (authorization IDs or roles), including DB2 administrative authorities (AU.3-DB2-14b). The criteria for the audit policy can include:

- Audit category (see table below)
- Schema name (for OBJMAINT and EXECUTE categories)
- Object Type (for OBJMAINT and EXECUTE categories)
- System administrative authorities (not allowed in the evaluated configuration, not supported by the RACF exit)
- Database administrative authorities (not allowed in the evaluated configuration, not supported by the RACF exit)

- Database name (not allowed in the evaluated configuration, used to qualify database administrative authorities)

Audit Category	Description
CHECKING	Generates IFCID 140 trace records for denied access attempts due to inadequate DB2 authorization and IFCID 83 trace records for RACF authentication failures
VALIDATE	Generates IFCID 55, 83, 87, 169, and 319 trace records for new or changed assignments of authorization IDs and IFCID 269 trace records for the establishment of trusted contexts or the switch of users in existing trusted contexts.
OBJMAINT	Generates IFCID 142 trace records when tables are altered or dropped.
EXECUTE	Generates IFCID 143 and 144 trace records for SQL statement and generates IFCID 145 records to trace bind time information about SQL statements that involve audited objects.
CONTEXT	Generates IFCID 23, 24, and 25 records.
SECMAINT	Generates IFCID 270 trace records for creating and altering trusted contexts, and IFCID 271 trace records for creating, altering, and dropping row permissions or column masks. Generates also IFCID 141 trace records for granting and revoking privileges or administrative authorities, but this record is not generated in the evaluated configuration, as privileges and administrative authorities are maintained through RACF.
SYSADMIN	Generates IFCID 361 trace records when an administrative authority, in the order of installation SYSADM, installation SYSOPR, SYSOPR, SYSCTRL, or SYSADM, satisfies the required privilege for performing an operation. This category is not allowed in the evaluated configuration as it is not supported by the RACF exit.
DBADMIN	Generates IFCID 361 trace records when an administrative authority, in the order of DBMAINT, DBCTRL, DBADM, PACKADM, SQLADM, system DBADM, DATAACCESS, ACCESSCTRL, or SECADM, satisfies the required privilege for performing an operation. This category is not allowed in the evaluated configuration as it is not supported by the RACF exit.

Table 28 – Audit categories

DB2-generated audit records can be extracted formatted and printed using the audit record evaluation tool (DSN1SMFP) (AU.3-DB2-15).

Audited tables also include those with the AUDIT attribute as well as all tables with row level security (AU.3-DB2-16).

7.6 Object reuse

7.6.1 Object reuse in DB2

DB2 manages its own objects. When a DB2 object is deleted, DB2 ensures that the space that has been occupied by those objects cannot be accessed by DB2 functions unless the space is allocated to another DB2 object and completely filled with the initial values for this new object (OR.1-DB2-1). This ensures that values stored in space allocated to DB2 objects that have been deleted cannot be accessed using DB2 functions until it is allocated to another DB2 object and has been prepared for reuse as part of this allocation.

DB2 stores its objects in z/OS data sets. Object reuse for data sets is provided by z/OS. Direct access by untrusted users to the data sets used by DB2 needs to be prohibited using the RACF access control functions for data sets.

8 Abbreviations, Terminology and References

8.1 Abbreviations

The abbreviations given in the Common Criteria standards [CC] and [CEM], the Protection Profile [DBMSPP] and the following apply to this Security Target.

ADMF	Asynchronous Data Mover Facility (Database Services)
APAR	Authorized Program Analysis Report
BCP	Base Control Program
BSDS	Bootstrap Data Set
CAF	Call Attachment Facility
CPACF	Central Processor Assist for Cryptographic Functions
DBRM	Data Base Request Module
DDF	Distributed Data Facility
DDM	Distributed Data Management
DFS	Data Facility Storage
DFSMD	Data Facility Storage Management System
DRDA	Distributed Relational Database Architecture
DSCF	System Services
DSN	Data Source Name
FMID	Function Modification Identifier
HCD	HCD Hardware Configuration Definition
ISPF	Interactivity System Product Facility
JAR	Java ARchive

JES2	Job Entry Subsystem
LDAP	Lightweight Directory Access Protocol
LOB	Large Object in DB2
MVS	Multiple Virtual Storage
PR/SM™	Processor Resource/Systems Manager™
RACF	Resource Access Control Facility
RAMAC	Random Access Memory Accounting System
RDBMS	Relational DBMS
RRS	Resource Recovery Service
RRSAF	Resource Recovery Services Attachment Facility
RVA	RAMAC Virtual Array
SAF	System Authorization Facility
SDSF	System Display and Search Facility
SMF	System Management Facility
SNA	Systems Network Architecture
SQL	Structured Query Language
TSO	Time Sharing Option
VUE	Value Unit Edition

8.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terminology defined in the [CC], the [CEM] and [DBMSPP] are also applicable to this document, unless redefined below.

The following glossary provides a short explanation of the DB2 database terms used throughout this document and points out different usage where appropriate:

Administrative Authority

A set of privileges often covering a related set of objects. Authorities often include privileges that are not explicit, have no name, and cannot be specifically granted.

Audit Policy

A set of criteria that determines the categories to be audited.

Buffer Pool

Buffer pools are areas of virtual storage in which DB2 temporarily stores pages of table spaces or indexes. When an application program accesses a row of a table, DB2 retrieves the page containing that row and places the page in a buffer. If the needed data is already in a buffer, the application program does not have to wait for it to be retrieved from disk, significantly reducing the cost of retrieving the page.

Collection

A collection of packages

Column

The vertical component of a table. A column has a name and a particular data type (for example, character, decimal, or integer).

Column mask

A database object that describes a specific column access control rule for a column.

Database

A set of DB2 structures that includes a collection of tables, their associated indexes, and the table spaces and index spaces in which they reside.

Database Role

A database entity available only in a trusted context that groups together one or more privileges. A role can own database objects, which helps eliminate the need for individual users to own and control database objects.

DB2 object

The DB2 objects are defined in section 7.3.3.1.

DB2 subject

DB subject further are z/OS users that are defined by the DB2 primary authorization ID. A DB2 subject is represented by a DB2 agent structure which represents requests coming from allied address spaces or external DRDA clients.

DB2 process

In DB2, the unit to which DB2 allocates resources and locks. Sometimes called an application process, a process involves the execution of one or more programs. The execution of an SQL statement is always associated with some process. The means of initiating and terminating a process are dependent on the environment.

DB2 process is mentioned in sections **Error! Reference source not found.** and 7.3.3.2.

Distinct type

A user-defined data type that is internally represented as an existing type (its source type), but is considered to be a separate and incompatible type for semantic purposes.

Function

A function is an operation denoted by a function name followed by zero or more operands that are enclosed in parentheses. It represents a relationship between a set of input values and a set of result values. The input values to a function are called arguments.

The types of functions are aggregate, scalar, and table. A built-in function is classified as an aggregate function or a scalar function. A user-defined function can be a column, scalar, or table function.

Index

An index is an ordered set of pointers to the data in a DB2 table. The index is stored separately from the table.

Java Archive

A file format that is used for aggregating many files into a single file.

Package

A package contains control structures used to execute SQL statements. Packages are produced during program preparation. The control structures can be thought of as the bound or operational form of SQL statements taken from a database request module (DBRM). The DBRM contains SQL statements extracted from the source program during program preparation. All control structures in a package are derived from the SQL statements embedded in a single source program.

Plan

An application plan relates an application process to a local instance of DB2, specifies processing options, and contains one or both of the following elements:

A list of package names

The bound form of SQL statements taken from one or more DBRMs

Primary authorization ID

The authorization identifier used to identify an application process to DB2 for z/OS.

RACF Profile

A collection of attributes belonging to a RACF object such as users.

Row

The horizontal component of a table. A row consists of a sequence of values, one for each column of the table.

Row Permission

A database object that describes a specific row access control rule for a table.

Schema

A schema is a collection of named objects. The objects that a schema can contain include distinct or built-in types, functions, stored procedures, sequences, and triggers. An object is assigned to a schema when it is created.

Sequence

A user-defined object that generates a sequence of numeric values according to user specifications.

Started Task

A pre-defined job of the z/OS operating system. As such it can represent a subject and it can have subject attributes. Attributes of started tasks can be represented in the RACF STARTED class or in the started procedures table of the ICHRIN03 module.

Storage Group

The description of a storage group names the group and identifies its volumes and the VSAM (virtual storage access method) catalog that records the data sets. The default storage group, SYSDEFLT, is created when you install DB2.

Stored Procedure

A stored procedure (sometimes called a procedure) is a routine that can be called to perform operations that can include both host language statements and SQL statements. Procedures are classified as either SQL procedures or external procedures. SQL procedures contain only SQL statements. External procedures reference a host language program, which may or may not contain SQL statements.

Subsystem or data sharing group

A distinct instance of DB2.

Table

All data in a DB2 database is presented in tables—collections of rows all having the same columns. A table that holds persistent user data is a base table. A table that stores data temporarily is a temporary table.

Tablespace

A set of volumes on disks holding data sets in which tables and indexes are actually stored.

Trigger

A trigger defines a set of actions that are executed when a delete, insert, or update operation occurs on a specified table. When such an SQL operation is executed, the trigger is said to be activated.

Trusted Context

A database entity based on a system authorization ID and a set of connection trust attributes.

View

A view is an alternate way of representing data that exists in one or more tables. A view can include all or some of the columns from one or more base tables.

8.3 References

[BSI-PP] Common Criteria (CC) Protection Profiles for IT products (Schutzprofile nach Common Criteria (CC) für IT-Produkte)
Location
https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/SchutzprofileProtectionProfiles/schutzprofileprotection-profiles_node.html

[CC] Common Criteria for Information Technology Security Evaluation,
Version 3.1R4, September 2012
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf

[CEM] Common Methodology for Information Technology Security Evaluation
Version 3.1R4, September 2012
Location http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R4.pdf

[DB2AG] DB2 v12 for z/OS Administration Guide
Document Number: SC27-8844

[DB2API] DB2 v12 for z/OS Application Programming and SQL Guide
Document Number: SC27-8845

[DB2CCG] DB2 v12 for z/OS Requirements for the Common Criteria
Document Number: SC27-8863

[DB2CR] DB2 v12 for z/OS Command Reference
Document Number: SC27-8848

[DB2IG] DB2 v12 for z/OS Installation and Migration Guide
Document Number: GC19-8851

[DB2INT] DB2 v12 for z/OS Introduction to DB2 for z/OS
Document Number: SC27-8852

[DB2ACMG] DB2 v12 for z/OS RACF Access Control Module Guide
Document Number: SC27-8858

[DB2WN] DB2 v12 for z/OS What's New
Document Number: GC27-8861

[DB2SQL] DB2 v12 for z/OS SQL Reference
Document Number: SC27-8859

[DB2UGR] DB2 v12 for z/OS Utility Guide and Reference
Document Number: SC27-8860

[DB2SECM] DB2 v12 for z/OS Managing Security
Document Number: SC27-8854

[DBMSPP] BSI-CC-PP-0088, Base Protection Profile for Database Management Systems.
V 2.12, March 23rd, 2017

[DRDA-V1] Open Group Technical Standard, DRDA Version 5 Vol. 1: Distributed Relational Database Architecture

[DRDA-V2] Open Group Technical Standard, DRDA Version 5 Vol. 2: Formatted Data Object Content Architecture

[DRDA-V3] Open Group Technical Standard, DRDA Version 5 Vol. 3: Distributed Data Management Architecture

[GUIDE] ISO/IEC TR 15446 Title: Information technology – Security techniques – Guide for the production of protection profiles and security targets, 2009

[PMLS] Planning for Multilevel Security and the Common Criteria
Document Number: GA22-7509-13
2012 edition

[RACFST] Security Target for RACF Element of z/OS Version 2, Release 2
Version 4.12
October 14, 2016

[ZOSST] Security Target for IBM z/OS Version 2 Release 2
Version 10.9
2014-08-28