

DB2 v9.1 for z/OS Security Target

Version 1.29

Status: Released

Last Update: 2012-07-31

atsec is a trademark of atsec GmbH

IBM, IBM logo, DB2 Version 9.1 for z/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

- Advanced Function Presentation
- AFP
- DFS
- DFSORT
- @server
- IBM
- Infoprint
- MVS
- PR/SM
- Print Services Facility
- Processor Resource/Systems Manager
- RACF
- VTAM
- z/Architecture
- z/OS
- z/VM
- zSeries

Intel and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States, other countries, or both.

Java and all Java-based products are trademarks of Sun Microsystems, Inc., in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

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

This document may be reproduced or distributed in any form without prior permission provided the copyright notice is retained on all copies. Modified versions of this document may be freely distributed provided that they are clearly identified as such, and this copyright is included intact.

Copyright (c) since 2005 by atsec GmbH and IBM Corporation or its wholly owned subsidiaries.

Document History

Version	Date	Summary	Author
1.29	2012-07-31	Removed confidentiality label, internal document history, and updated copyright notice, for release – no content/version change	Alejandro Masino

Table of Content

1	Introduction	7
1.1	ST reference	7
1.2	TOE reference	7
1.3	TOE overview	7
1.4	TOE description	9
1.4.1	Structure of DB2.....	9
1.4.2	TOE boundary and interfaces	14
1.4.3	Software security function summary	14
1.4.4	Configurations	16
2	Conformance claims	19
2.1	CC conformance claim	19
2.2	Protection Profile claims	19
2.2.1	Controlled Access Protection Profile ([CAPP]).....	19
2.2.2	U.S. Government Protection Profile for DBMS in Basic Robustness Environments ([BR-DBMSPP]).....	19
2.3	Rationale for Demonstrable Conformance	21
3	Security problem definition	22
3.1	Introduction	22
3.2	Threats.....	22
3.3	Organizational security policies	22
3.4	Assumptions	23
3.5	Rationale for Demonstrable Conformance	23
3.5.1	Threats	24
3.5.2	Organizational Security Policies.....	24
3.5.3	Assumptions.....	24
4	Security objectives	25
4.1	Security objectives for the TOE	25
4.2	Security objectives for the operational environment.....	26
4.3	Rationale for the Security Objectives	26
4.4	Rationale for Demonstrable Conformance	27
4.4.1	Security Objectives for the TOE	27
4.4.2	Security Objectives for the Operational Environment	28
5	Extended components definition.....	29
6	Security requirements	30
6.1	TOE security functional requirements	30
6.1.1	Security audit (FAU)	37

6.1.2	User data protection (FDP)	41
6.1.3	Identification and authentication (FIA).....	44
6.1.4	Security management (FMT).....	46
6.1.5	Protection of the TOE security functions (FPT).....	49
6.1.6	TOE Access (FTA)	49
6.2	Security Requirements for the IT Environment	50
6.2.1	IT Environment (FIT)	50
6.3	Security Functional Requirements Rationale	51
6.3.1	Internal consistency and mutual support of SFRs.....	51
6.3.2	Coverage	54
6.3.3	Sufficiency	55
6.3.4	Security requirements dependency analysis.....	55
6.3.5	Rationale for Demonstrable Conformance	57
6.4	TOE security assurance requirements	58
6.5	Security Assurance Requirements Rationale.....	58
6.6	TOE Summary Specifications Rationale	58
6.6.1	Security functions justification	58
7	TOE summary specification	62
7.1	Overview of the TOE architecture	62
7.1.1	Main trusted subsystems of the evaluated configuration	63
7.2	Identification and authentication	64
7.2.1	Authentication function	64
7.2.2	Special handling in DB2	64
7.2.3	Trusted connections	64
7.3	Access control	65
7.3.1	Access control principles.....	65
7.3.2	Protected resources of DB2	66
7.3.3	Mandatory access control (Labeled Security Mode only)	66
7.3.4	Discretionary access control in DB2	67
7.3.5	DB2 internal access checking	82
7.4	Communication security in z/OS	82
7.5	Security management.....	82
7.5.1	Security management in z/OS.....	82
7.5.2	Security management of DB2	82
7.5.3	DB2 user attributes and user roles and database roles.....	83
7.5.4	Trusted connections and database roles	85
7.6	Auditing.....	85

7.6.1	Auditing in DB2.....	85
7.7	Object reuse	87
7.7.1	Object reuse in z/OS	87
7.7.2	Object reuse in DB2	87
7.8	TOE self-protection.....	87
7.8.1	Protection of DB2 code and data structures	87
8	Abbreviations, Terminology and References.....	88
8.1	Abbreviations	88
8.2	Terminology	89
8.3	References	91

1 Introduction

1.1 ST reference

Title:	DB2 v9.1 for z/OS Security Target
Version:	1.29
Status:	Final
Date:	2012-07-31
Sponsor:	IBM Corporation
Developer:	IBM Corporation
Keywords:	IBM DB2 for z/OS; relational database management system (DBMS)

1.2 TOE reference

The Target of Evaluation (TOE) is the IBM DB2 Version 9.1 for z/OS Version 1 Release 10.

1.3 TOE overview

The Target of Evaluation (TOE) consists of:

- The “IBM z/OS Version 1 Release 10 (z/OS V1R10)” operating system, including the Resource Access Control Facility (RACF) which is used as the evaluated platform
- The “IBM DB2 Version 9.1 for z/OS” (DB2 9), which is built upon this platform.

This Security Target (ST) builds on the z/OS Security Target [ZOSST], which refers to the evaluated “IBM z/OS Version 1 Release 10” operating system.

DB2 9 is a relational database management system that operates as a subsystem of z/OS. DB2 is implemented by a set of address spaces plus a set of utilities.

The TOE is a combination of a platform (here z/OS) and an application (here DB2). Thus TOE means always DB2 and z/OS in this ST. For z/OS usually “z/OS platform” is used and for the application “DB2”.

DB2 9 operates as a subsystem of z/OS and uses the security functionality of z/OS. Thus this security target is an extension of the z/OS V1R10 security target where the additional security functionality of DB2 9 is described. To avoid redundancy with the z/OS security target, this document only describes the additional or modified security functionality introduced by DB2 9.

DB2 9 is a component that uses and extends the functionality of z/OS V1R10. This evaluation is based on the evaluation of the z/OS V1R10 itself and will therefore only claim security functionality provided by DB2 9.

The z/OS Security Target [ZOSST] contains, in section 1.2 “TOE overview”, an introduction about the z/OS V1R10 operating system TOE that is considered in this evaluation.

DB2 for z/OS is IBM's flagship database management system, designed to efficiently and cost-effectively deliver information to enterprise-class e-business applications and leveraging the capacity and processing power of IBM  zSeries and z/OS.

Version 9.1 of DB2 has introduced enhancements to performance, reliability/availability and security, breaking barriers in key areas of database deployment.

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 9 for z/OS provides security options for e-business and high security with multilevel security and row-level security as well as high security, more granularity and more information for additional flexibility in applications and SQL, and encryption capabilities.

In addition DB2 9 for z/OS improves access control by database roles in a trusted context which provides the flexibility for managing context-specific privileges and simplifies the processing of authorization. Improved filtering makes auditing more usable and the Secure Sockets Layer (SSL) data encryption on networks is more secure.

The target of this evaluation (TOE) is a well-chosen combination of IBM products around DB2 and z/OS (see section 1.4.4 of this ST), which together provide a powerful DBMS with security functions fulfilling the requirements of the U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.2. ([BR-DBMSPP]) and the Controlled Access Protection Profile ([CAPP]). In the configuration chosen for this evaluation, DB2 uses the access control and security management services provided by the Resource Access Control Facility (RACF) of z/OS for discretionary access controls and to implement multilevel security controls down to the granularity of individual rows in a database.

In the evaluated configuration the TOE provides access control functions for z/OS and DB2 using RACF as the central access control module. Access rights for both z/OS and DB2 objects are therefore managed using the same interface provided by RACF. Access controls defined by the SQL GRANT and REVOKE commands are not relevant and therefore ignored in the evaluated version of the TOE with access control to the DB2 objects provided by RACF.

The TOE also implements mandatory access control for both z/OS and DB2 objects. In DB2 mandatory access control is implemented by a dedicated column in each table that contains the sensitivity label of the row. This column is maintained by the TOE and can not be altered by a user unless he has the specific privilege to overwrite labels.

To operate a mainframe system which deploys the products constituting this TOE in either a CAPP or Labeled Security Mode of operation, the products must be installed in their evaluated version and configured in a secure manner as described in the directions delivered with the media and the accordant guides listed in the [ZOSST] and especially for DB2 9, “DB2 Version 9.1 for z/OS Administration Guide” ([DB2AG]).

This security target (ST) documents the security characteristics of the TOE described above in the Labeled Security and CAPP modes of operation.

In this ST, the TOE consists of one instance of z/OS V1R10 running on an abstract machine as the sole operating system exercising full control over it, and DB2 9 running on top of z/OS V1R10.

Multiple instances of the TOE may be connected in a basic sysplex or in a parallel sysplex, sharing their RACF database and acting like a single system. This functionality is provided by z/OS V1R10 (see [ZOSST]), DB2 relies on the mechanisms provided by the underlying operating system.

The required runtime environment for the z/OS V1R10 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 DB2 9.

User identification and authentication and parts of access control to DB2 objects are provided by the Resource Access Control Facility (RACF), a z/OS Security Server component that is used by different services as the central instance for identification and authentication and for access control decisions. z/OS V1R10 and DB2 9 come with management functions that allow configuring the TSF and tailor them to the customer’s needs.

Some elements that have been included in the TOE do not provide security functions. These elements run in authorized mode, so they could compromise the TOE if they do not behave properly. Because these elements are essential for the operation of many customer environments, the inclusion of these

elements subjects them to the process of scrutiny during the evaluation and ensures that they may be used by customers without affecting the TOE's security status.

In its evaluated configuration, the TOE allows two modes of operation: Labeled Security mode and CAPP-mode. In both modes, the same software elements are used. The two modes have different RACF settings with respect to the use of security labels. All other configuration parameters are identical in the two modes.

Throughout this Security Target, all claims that are valid for the Labeled Security mode only are marked accordingly.

1.4 TOE description

The Target of Evaluation (TOE) is the IBM DB2 Version 9.1 for z/OS (DB2 9) on the IBM z/OS Version 1 Release 10 (z/OS V1R10) operating system, including the Resource Access Control Facility (RACF).

The security description and configuration of the z/OS V1R10 operating system is provided in the z/OS Security Target [ZOSST] section 1.3 "TOE description", and is considered in this evaluation. Only the DB2 specific functionality is described below.

1.4.1 Structure of DB2

DB2 9 is a relational database management system that operates as a subsystem of z/OS. DB2 is implemented by a set of address spaces plus a set of utilities.

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

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

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

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

A requester using DRDA connects to an application server or database server. DRDA uses Distributed Data Management (DDM) and Formatted Data Object Content Architecture (FD:OCA) as part of the underlying architecture of DRDA. DDM is the communication language used for message interchange systems. FD:OCA is used to exchange user data among like or unlike systems. This allows external users to connect to DB2 and operate on DB2 databases.

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

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

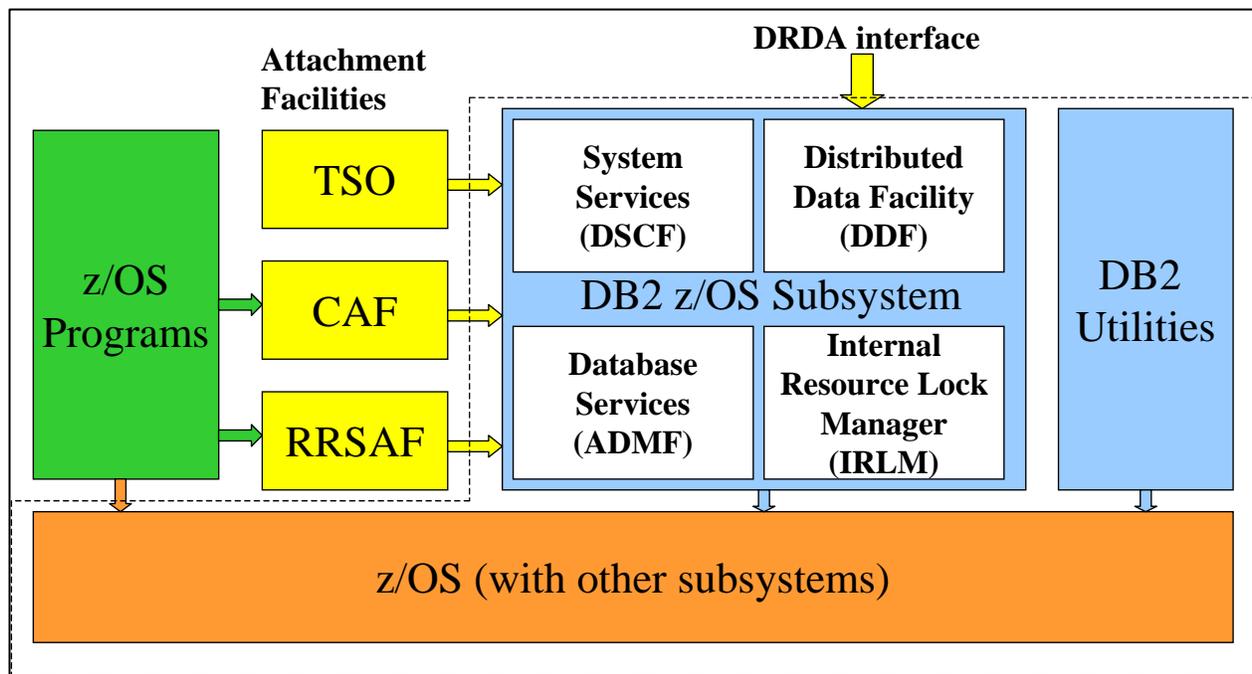


Figure 1: Basic structure of DB2 for z/OS showing TOE structure with TOE boundary

The blue boxes in this figure represent the trusted parts of DB2, the yellow boxes represent those parts of the attachment facilities of DB2 executing in the user's address space or connections using the network interface. The brown box represents the z/OS system as the platform of this TOE. 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.

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 DB2 security functions

DB2 is operating on top of the IBM z/OS V1R10 operating system and uses functions of this operating system to protect itself from untrusted users that attempt to tamper with objects managed by DB2. In addition, DB2 uses functions provided by the operating system to implement the following security functions:

Identification and authentication

DB2 relies on the identification and authentication performed by z/OS. When checking for the user's right to use authorities managed by DB2, the database management system uses the ID of the user verified by z/OS.

Additionally, DB2 can establish a trusted connection with a user or system when a trusted context matches the characteristics of the connection, based on the user ID and connection trust attributes (e.g. IP address, domain name or SERVAUTH security zone name for a remote client, the job or task name for a local client). A trusted context allows the association of the trusted connection with a database role, a different user or a security label (in Labeled Security mode) for access control.

Object access control

In the evaluated configuration, DB2 uses RACF to check for and manage access control to DB2 objects. DB2 internal access controls based on the GRANT and REVOKE SQL statements will not be effective in the evaluated configuration.

In the case of a trusted connection, access control also includes object ownership rules based on database roles. A database role can be assigned to the DB2 process by a trusted context.

In Labeled Security mode, mandatory access control is in effect: DB2 then uses the labels defined in the RACF profiles related to DB2 objects as well as the DB2-managed labels of rows in tables. In any case, the label-based access checks for mandatory access control are performed using RACF. In the case of a trusted connection, the default security label defined for the related trusted context, if any, is assigned to the DB2 process.

Audit

The audit requirements are implemented using a mix of SMF records generated by RACF and the DB2 internal trace.

TSF management

In the evaluated configuration DB2 uses the functions provided by RACF to manage user profiles as well as the profiles related to DB2 objects. Access to authorities of DB2 objects is controlled by those profiles. Labels for rows in tables are assigned when they are created using the current label of the user that creates the row. The current label of the user is maintained by RACF.

TOE self protection

DB2 uses the protection mechanisms of z/OS with RACF to protect its address space, functions and objects from unauthorized access and manipulation.

1.4.1.2 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
 - Distinct type – not in evaluated configuration
 - Sequence
- Trusted context

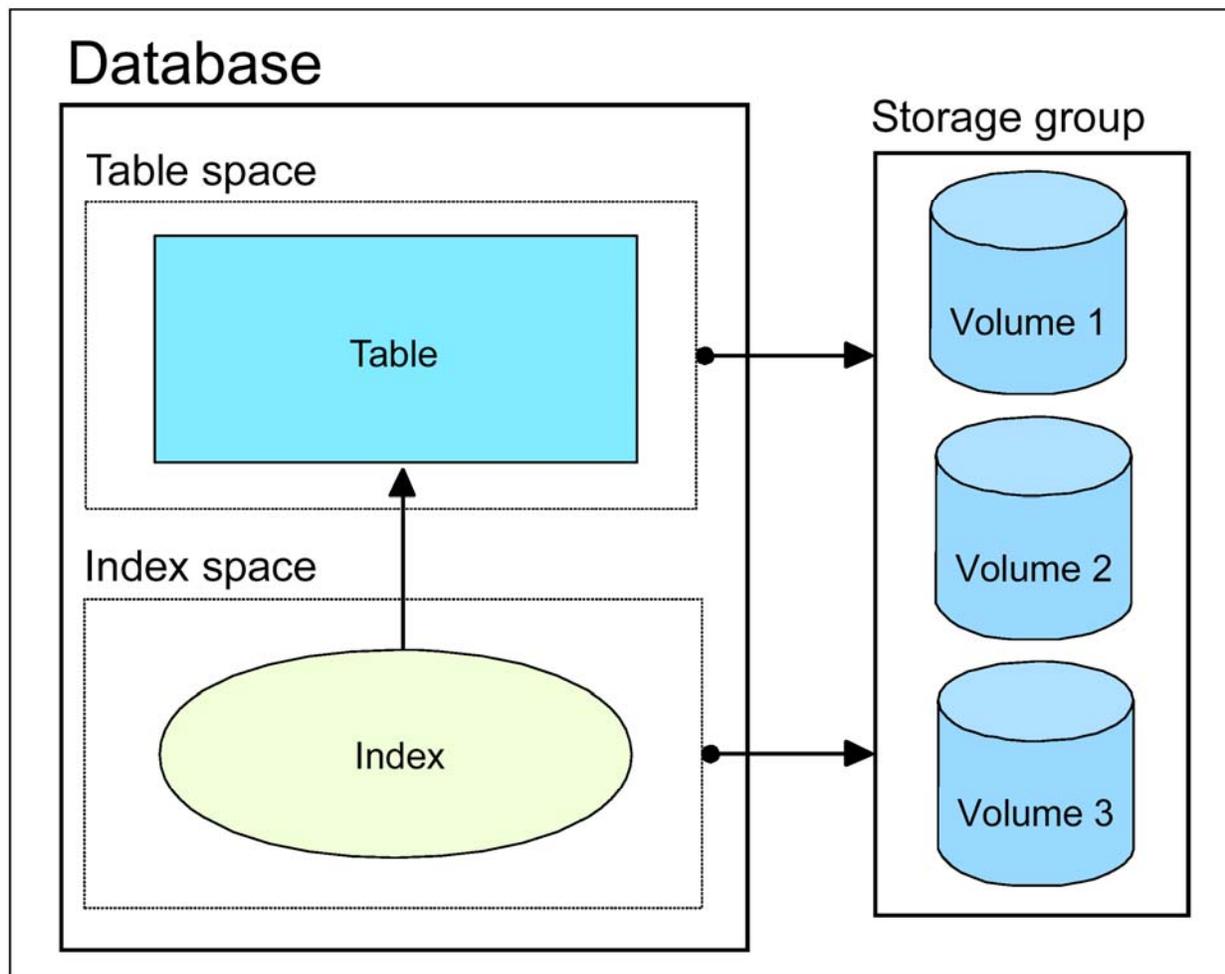


Figure 2: (Simplified) structure of a DB2 database

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

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.

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.

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.

1.4.1.4 Application processes and transactions

Many different types of programs access DB2 data: user-written applications, SQL statements that users enter dynamically, and even utilities. The single term that describes any type of access to DB2 data is called an application process. All SQL programs run as part of an application process. An application process involves running one or more programs. Different application processes might involve running different programs, or different runs of the same program.

When an application interacts with a DB2 database, a transaction begins. A transaction is a sequence of actions between the application and the database that begins when data in the database is read or written. A transaction is also known as a unit of work.

1.4.1.5 The authorization hierarchy

Users (as identified by an authorization ID) can successfully execute SQL statements only if they have the authority to perform the specified operation. The two forms of authorization are administrative authority and privileges.

Privileges

Privileges are those activities that a user is allowed to perform. Authorized users can create objects, have access to objects that they own, and can pass on privileges on the objects that they own to other users by using the GRANT statement (although this is not allowed in the evaluated configuration).

Administrative Authority

An administrative authority is an administration role that can be granted to users in order to perform administrative tasks on DB2. Administrative authorities are composed by a specific group of privileges and fall into the categories of system, database, and collection authorities.

Administrative authorities form a hierarchy. The highest ranking administrative authority is SYSADM. Each level of authority includes the privileges of all lower-ranking authorities.

System authorities (ranked from highest to lowest) include:

- SYSADM: System administration authority includes all DB2 privileges (except for a few that are reserved for installation), which are all grantable to others.
- SYSCTRL: System control authority includes most SYSADM privileges; it excludes the privileges to read or change user data.
- SYSOPR: System operator authority includes the privileges to issue most DB2 commands and end any utility job.

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.

For a graphical view of the DB2 authorization hierarchy see **Figure 3** in chapter 6 of this document.

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 z/OS code operating with the above mentioned privileges. Due to the strong interrelation between DB2 and large parts of z/OS (especially RACF) the TOE includes both DB2 Version 9.1 and z/OS Version 1 Release 10.

z/OS Version 1 Release 10 (including RACF) has been evaluated previously at the EAL4+ level and the results of this evaluation will be reused. The basic security requirements and security functions of z/OS are defined in the z/OS Security Target document [ZOSST] and are therefore not repeated but only referenced here. The DB2 specific security requirements and functions are described throughout this document.

Figure 1 above shows the components of the TOE and the boundary of the trusted part of the TOE as a dotted line. The interfaces are shown as arrows where the yellow arrows indicate external interfaces of the DB2 component, the orange arrow indicates the external interfaces of z/OS and the blue arrows indicate internal interfaces the DB2 subsystem uses for requesting services of z/OS.

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
- Mandatory access control and support for security labels
- Audit
- Object re-use functionality
- Communication security
- Security management
- TSF protection

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 z/OS platform provides user identification and authentication. The z/OS user ID and its associated attributes and user roles are used by DB2 for z/OS 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 done through RACF.

1.4.3.2 Discretionary access control in DB2

In addition to the access control mechanisms provided by the z/OS platform (see [ZOSST]), 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 DB2 role, 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. 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 also uses RACF to check for and manage 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, which is a database entity based on a system authorization ID and a set of connection trust attributes.

1.4.3.3 Mandatory access control and support for security labels (Labeled Security Mode only)

The functionality provided by the z/OS platform is described in [ZOSST].

DB2 can use the mandatory access control based on security labels from the z/OS platform to protect access to certain DB2 objects, such as tables. In addition, DB2 provides mandatory access control to the granularity of rows within tables.

With row-level security active a table has a dedicated column that contains the security label of each row in the table. This row is maintained by the TOE such that the label of the row contains the highest security label of data written into that row. DB2 uses RACF to check that users attempting to read or write to a row are operating with a security label that allows the requested operation in accordance with rules for mandatory access control (a default security label can be assigned to the user process in a trusted connection). Those checks are performed in addition to the discretionary access checks performed.

1.4.3.4 Audit

In addition to the audit functionality provided by the z/OS platform (see [ZOSST]), 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.

1.4.3.5 Object re-use functionality

The functionality provided by the z/OS platform is described in [ZOSST]

DB2 for z/OS implements object reuse for all database objects by clearing all objects prior to re-use. All DB2 objects 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. z/OS data sets are protected from direct access by untrusted users by the z/OS platform. This prohibits bypassing the DB2 object reuse functions.

1.4.3.6 Communication security

DB2 does not provide specific network security functions. For data transmission and DRDA remote access, the z/OS platform provides a variety of choices to protect communication links, such as IPSec, SSL, or AT-TLS (see [ZOSST]).

1.4.3.7 Security management

In addition to the security management functions provided by the z/OS platform, which includes management of the system's general security options, user management, and management of the access

control mechanisms of z/OS (see [ZOSST]), 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.

1.4.3.8 TSF protection

The functionality provided by the z/OS platform is described in [ZOSST]. DB2 fully relies on the TSF protection mechanisms provided by the z/OS platform.

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 V9 Package, which includes:
 - One of the two versions of DB2 Version 9.1 for z/OS:
 - the standard DB2 Version 9.1 for z/OS (program number 5635-DB2)
 - DB2 Version 9.1 for z/OS VUE (value unit edition) (program number 5697-P12), which delivers a one-time-charge price metric for Eligible Workloads.
 - DB2 Utilities Suite for z/OS, V9.1 (program number 5655-N97)
- The Common Criteria Evaluated Base for z/OS V1R10 Package, as specified in the Security Target for IBM z/OS Version 1 Release 10 ([ZOSST]).

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

In addition any software outside the TOE may be added without affecting the security characteristics of the system, if it has the characteristics described in [ZOSST], section 1.3.3.1.

Both versions of DB2 version 9.1 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 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 9 for z/OS VUE license.

In case the licensing option is chosen, DB2 Version 9.1 for z/OS VUE requires running in a logical partition (LPAR) on z/OS V1R10 configured as zNALC (System z New Application License Charges).

For the purpose of this evaluation, DB2 Version 9.1 for z/OS (program number 5635-DB2) will be used.

Additionally, both versions of DB2 version 9.1 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:

- HIY9910 IMS Attach
- JDB9912 JDBC/SQLJ
- JDB9917 ODBC
- JDB991X XML Extender

1.4.4.1.1 z/OS installation options and restrictions

The z/OS installation options and restrictions are provided by the z/OS platform as described in [ZOSST] section 1.3.3.1.

1.4.4.1.2 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 HIY9910)
- Java Archives (JAR)
- JDBC/SQLJ (FMID JDB9912)
- Kerberos
- ODBC/CLI (FMID JDB9917)
- PassTickets
- Secondary authorization IDs
- Sign-on authorization IDs
- SNA™ connections
- Unified debugger
- XML Extender (FMID JDB991X)
- z/OS ODBC interface to SQL
- DB2 Web Services
- MQseries user-defined functions
- User exit routines
- mSys for Setup DB2 Customization Center

The default values of some fields on the following panels cannot be accepted:

- Protection panel DSNTIPP
- Distributed data facility panel 1: DSNTIPR

In the DB2 configuration package, routine, and statement caching must be turned off.

1.4.4.2 Hardware configurations

This TOE allows the use of all hardware and hardware configurations as defined in [ZOSST], section 1.3.4.

1.4.4.3 TOE guidance

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

- DB2 Version 9.1 Common Criteria Guide
- DB2 Version 9.1 for z/OS What's New? (GC18-9856-02)
- DB2 Version 9.1 for z/OS Introduction to DB2 for z/OS (SC18-9847-02)
- DB2 Version 9.1 for z/OS Installation Guide (GC18-9846-05)
- DB2 Version 9.1 for z/OS Administration Guide (SC18-9840 -03)
- DB2 Version 9.1 for z/OS Command Reference (SC18-9844-03)
- DB2 Version 9.1 for z/OS RACF Access Control Module Guide (SC18-9852 -01)
- DB2 Version 9.1 for z/OS Data Sharing: Planning and Administration (SC18-9845-02)
- DB2 Version 9.1 for z/OS Reference for Remote DRDA Requesters and Servers (SC18-9853-02)
- DB2 Version 9.1 for z/OS Codes (GC18-9843-03)
- DB2 Version 9.1 for z/OS Messages (GC18-9849-03)
- DB2 Version 9.1 for z/OS Application Programming Guide and Reference for Java™ (SC18-9842-03)
- DB2 Version 9.1 for z/OS Application Programming and SQL Guide (SC18-9841-03)
- DB2 Version 9.1 for z/OS SQL Reference (SC18-9854-05)
- DB2 Version 9.1 for z/OS Utility Guide and Reference (SC18-9855-03)

2 Conformance claims

2.1 CC conformance claim

This ST is [CC] *Part 2 extended* and *Part 3 conformant*, with a claimed Evaluation Assurance Level of EAL4, augmented by ALC_FLR.3. The Common Criteria version 3.1 has been taken as the basis for this conformance claim.

2.2 Protection Profile claims

This Security Target claims **demonstrable conformance** with the following protection profiles:

- Controlled Access Protection Profile ([CAPP]) Version 1.d, October 1999.
- U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments ([BR-DBMSPP]), Version 1.2, July 2007.

Both protection profiles are listed on the NIAP web site as validated profiles. See <http://www.niap-ccevs.org/cc-scheme/pp> for more information.

2.2.1 Controlled Access Protection Profile ([CAPP])

The CAPP was developed by the “Information System Security Organization” of the National Security Agency of the United States of America based on Version 1 of the Common Criteria. Version 1.d was updated for compatibility with CC version 2.0.

As this protection profile is based on an earlier version of the Common Criteria, some SFRs and SARs defined in this PP have been modified to meet the requirements of Common Criteria version 3.1:

- The security functional requirements FPT_RVM.1 and FPT_SEP.1 included in CAPP have been omitted, since they are addressed in CC 3.1 by the inclusion of ADV_ARC.1.
- CAPP includes the security assurance requirements for the EAL3 assurance level of the CC Version 2.0. The security assurance requirement definition in this ST is considered a superset of the assurance requirements defined in the protection profile, therefore the minimum evaluation assurance level required in the protection profile is fulfilled.
- CAPP includes the security functional requirement FPT_AMT.1. In CC 3.1 Revision 3 this SFR has been replaced by FPT_TEE.1. This security functional requirement is implemented by the IT environment supporting z/OS. See section 4.4.1.4 in [ZOSST] for more information.
- CAPP includes the security functional requirements FAU_SAR.3 and FAU_STG.4. In CC 3.1 the wording of these SFRs has been changed but this was not updated in [ZOSST]. Since only the wording is different but not the content, i.e. for FAU_SAR.3 performing searches is a method of selection and in FAU_STG.4 auditable events was replaced by audited events, referencing to these SFRs is determined to be sufficient and the SFRs are not repeated and modified in this ST.

2.2.2 U.S. Government Protection Profile for DBMS in Basic Robustness Environments ([BR-DBMSPP])

The BR-DBMSPP was developed by the “Information Assurance Directorate” and sponsored by the National Security Agency and the National Information Assurance Partnership (NIAP) of the United States of America based on Version 2.x of the Common Criteria.

Version 1.2 of the protection profile was adapted for CC version 3.1; however, [BR-DBMSPP] still contains some inconsistencies that would cause a failure in the evaluation of the ASE class.

The table below shows the inconsistencies encountered by BSI and an explanation of the approach taken in this Security Target for each issue:

	Inconsistency	Action taken
1.	<p>In section 4.3, the following are security objectives for the TOE that have not been traced back by at least one SFR:</p> <ul style="list-style-type: none"> • O.ADMIN_GUIDANCE • O.CONFIGURATION_IDENTIFICATION • O.DOCUMENTED_DESIGN • O.INTERNAL_TOE_DOMAINS • O.PARTIAL_FUNCTIONAL_TEST • O.PARTIAL_SELF_PROTECTION • O.VULNERABILITY_ANALYSIS <p>As specified in [CEM, ASE_REQ.2.11] this is not allowed.</p>	<p>An application note is added in section 4.3 to clarify that these security objectives are implicitly covered by the EAL claimed in this ST.</p>
2.	<p>In section 6.1.4.5, the following SFRs are not drawn correctly from CC Part 2 (the wording corresponds to CC 2.3):</p> <ul style="list-style-type: none"> • FAU_SEL.1.1 • FMT_REV.1.1(1) • FMT_REV.1.1(2) 	<p>Since only the wording is different but not the content, the SFRs have been adjusted to match the wording in CC 3.1.</p>
3.	<p>Extended Component definition is not complete, there are no dependencies defined.</p> <ul style="list-style-type: none"> • FAU_GEN_(EXT).2 • FMT_MSA_(EXT).3 • FPT_TRC_(EXT).1 • FTA_TAH_(EXT).1 • FIT_PPC(EXT).1 	<p>The list of dependencies included in section 6.5 of [BR-DBMSPP] for each SFR matches the ones defined in CC Part 2 for the components the extended components are based on. The ST author understands that as changes in the extended components are minimal, they don't affect the dependencies on other SFRs.</p> <p>The only exception is FIT_PPC(EXT).1 which is a new security functional component that does not have a counterpart in CC Part 2. However, it is solely included for requiring an evaluated underlying platform for the TOE, therefore the ST author concludes that no dependency is necessary.</p>
4.	<p>In section 6.5 "The Rationale for Satisfying all Dependencies" is not consistent with section 5.1:</p> <ul style="list-style-type: none"> • FAU_GEN_(EXT).2 • FDP_ACC.1 • FMT_MSA_(EXT).3 • FPT_TRC_(EXT).1 	<p>The rationale for SFR dependencies for these particular SFR takes into account the definitions provided by this ST per action taken in issue 3.</p>
5.	<p>In section 3.2, table 3, the rationale for not including Basic Robustness policies wrongly considers OSPs as threats ("This threat is not applicable to the TOE...").</p>	<p>An application note is added in section 3.3 to clarify this inconsistency.</p>

For Basic Robustness systems, [BR-DBMSPP] requires EAL2 augmented by ALC_FLR.2. The security assurance requirement definition in this ST is considered a superset of the assurance requirements defined in the protection profile, therefore the minimum evaluation assurance level required in the protection profile is fulfilled.

2.3 Rationale for Demonstrable Conformance

This ST claims demonstrable conformance to [CAPP] and [BR-DBMSPP], which is allowed by both protection profiles.

Although the ST includes completely the security problem definition, the security objectives for the TOE and the security functional requirements for both protection profiles, and claims conformance to an EAL that provides complete coverage for the assurance requirements stated in both protection profiles, according to the [CC], the existence of a disjoint set of assumptions and security objectives for the environment requires that the claim against both protection profiles is of demonstrable conformance.

The demonstrable conformance rationale for the security problem definition, security objectives and security functional requirements (as explained in Appendix D.3 of [CC] part 1) is provided in the appropriate section of the ST:

- Section 3.5 "Rationale for Demonstrable Conformance" for the security problem definition.
- Section 4.4 "Rationale for Demonstrable Conformance" for security objectives of the TOE and security objectives for the operational environment.
- Section 6.3.5 "Rationale for Demonstrable Conformance" for security functional and assurance requirements

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 U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.2. ([BR-DBMSPP]) and the Controlled Access Protection Profile ([CAPP]). The Assets, Assumptions, Threats and Organizational Security Policies of these Protection Profiles are assumed here, together with extensions defined in sections 3.1 through 3.4 of the z/OS Security Target [ZOSST]. In the following sub-sections, only extensions to the different sections are listed. The titles of the chapters that are not extended are cited here for completeness.

3.2 Threats

This Security Target includes all threats defined in [BR-DBMSPP]. Note that [CAPP] does not define any threats as all security objectives are derived from the statement of Organizational Security Policy in that protection profile. There are no additional threats defined in this ST.

The category of threat agents in [ZOSST] section 3.2 and the description of the threat model in [BR-DBMSPP] are applicable to this ST.

The following table shows the threats defined in [BR-DBMSPP]:

Name	Defined in
T.ACCIDENTAL_ADMIN_ERROR	[BR-DBMSPP]
T.MASQUERADE	[BR-DBMSPP]
T.POOR_DESIGN	[BR-DBMSPP]
T.POOR_IMPLEMENTATION	[BR-DBMSPP]
T.POOR_TEST	[BR-DBMSPP]
T.RESIDUAL_DATA	[BR-DBMSPP]
T.TSF_COMPROMISE	[BR-DBMSPP]
T.UNAUTHORIZED_ACCESS	[BR-DBMSPP]
T.UNIDENTIFIED_ACTIONS	[BR-DBMSPP]

Table 1: Threats

3.3 Organizational security policies

This Security Target includes all Organizational Security Policies defined in [BR-DBMSPP], [CAPP], and section 3.3 “Organizational security policies” of the z/OS Security Target [ZOSST]. There are no additional OSP defined in this ST.

The following table shows the OSP defined in [BR-DBMSPP], [CAPP] and [ZOSST]:

Name	Defined in
P.AUTHORIZED_USERS	[ZOSST] copied from [CAPP]
P.NEED_TO_KNOW	[ZOSST] copied from [CAPP]
P.ACCOUNTABILITY	[BR-DBMSPP] and [ZOSST] copied from [CAPP]
P.ROLES	[BR-DBMSPP]
P.CLASSIFICATION (Labeled Security Mode only)	[ZOSST]

Table 2: Organizational security policies

Note: [BR-DBMSPP] describes in section 3.2, table 3 the basic robustness policies that are not applicable to the TOE (P.ACCESS_BANNER and P.CRYPTOGRAPHY). When the rationale states “This threat is not applicable to the TOE” it should say “This policy is not applicable to the TOE”. This is a known inconsistency in the protection profile.

3.4 Assumptions

This Security Target includes all assumptions defined in [BR-DBMSPP], [CAPP] and section 3.4 “Assumptions” of the z/OS Security Target [ZOSST]. There are no additional assumptions defined in this ST.

The following table shows the assumptions defined in [BR-DBMSPP], [CAPP] and [ZOSST]:

Name	Defined in
A.LOCATE	[ZOSST] copied from [CAPP]
A.PROTECT	[ZOSST] copied from [CAPP]
A.MANAGE	[ZOSST] copied from [CAPP]
A.NO_EVIL_ADM (equivalent to A.NO_EVIL in [BR-DBMSPP])	[BR-DBMSPP] and [ZOSST] copied from [CAPP]
A.COOP	[ZOSST] copied from [CAPP]
A.PEER	[ZOSST] copied from [CAPP]
A.CONNECT	[ZOSST] copied from [CAPP]
A.CLEARANCE (Labeled Security Mode only)	[ZOSST]
A.SENSITIVITY (Labeled Security Mode only)	[ZOSST]
A.NO_GENERAL_PURPOSE	[BR-DBMSPP]
A.OS_PP_VALIDATED	[BR-DBMSPP]
A.PHYSICAL	[BR-DBMSPP], similar to A.LOCATE and A.PROTECT together.

Table 3: Assumptions

3.5 Rationale for Demonstrable Conformance

The security problem definition provided in this ST is a superset of each of the security problems defined in [BR-DBMSPP], [ZOSST] and [CAPP], that is, all sets of threats, organizational security policies and assumptions defined in the cited protection profiles and the ST for z/OS are completely included. Even more, the security problem definition does not include any other additional threat, organizational security policy or assumption, so the security problem definition is the union of the security problems defined in the cited documents.

The following sections provide the rationale to justify that the security problem definition specified in this ST is more restrictive than the security problem definition specified in each protection profile claimed, and

that the resulting sets of threats, organizational security policies and assumptions are consistent and do not contradict to each other.

3.5.1 Threats

As described in section 3.2, all threats included in this ST are derived from [BR-DBMSPP]; security objectives in [ZOSST] and [CAPP] only enforce Organizational Security Policies (OSPs).

The set of threats is consistent with the Organizational Security Policies because:

- T.ACCIDENTAL_ADMIN_ERROR, T.POOR_DESIGN, T.POOR_IMPLEMENTATION, T.POOR_TEST and T.UNIDENTIFIED_ACTIONS have no OSP with similar meaning and therefore contribute to a more restrictive security problem definition.
- T.MASQUERADE and T.UNAUTHORIZED_ACCESS have similarities with P.AUTHORIZED_USERS; their definitions are supplemental and do not contradict to each other.
- T.RESIDUAL_DATA and T.TSF_COMPROMISE have similarities with P.NEED_TO_KNOW; their definitions are supplemental and do not contradict to each other.

3.5.2 Organizational Security Policies

As described in section 3.3, all Organizational Security Policies included in this ST are derived from [ZOSST], [CAPP] and [BR-DBMSPP]. The resulting set of Organizational Security Policies maintains its consistency and is supplemental to the threats defined in [BR-DBMSPP] as follows:

- P.AUTHORIZED_USERS and P.NEED_TO_KNOW defined in [ZOSST] (or [CAPP] respectively) are similar in meaning to the set of threats defined in [BR-DBMSPP].
- P.ACCOUNTABILITY exists both in [CAPP] and [BR-DBMSPP] with equivalent definitions.
- P.CLASSIFICATION defined in [ZOSST] limits access to information based on sensitivity (for Labeled Security Mode), contributing to a more restrictive security problem definition.
- P.ROLES defined in [BR-DBMSPP] requires an authorized administrator role, contributing to a more restrictive security problem definition.

3.5.3 Assumptions

As described in section 3.4, all assumptions included in this ST are derived from [ZOSST], [CAPP] and [BR-DBMSPP]. The resulting set of assumptions provides a more restrictive security problem definition for Basic Robustness:

- A.NO_EVIL defined in [BR-DBMSPP] is equivalent to A.NO_EVIL_ADM defined in [CAPP]
- A.NO_GENERAL_PURPOSE and A.OS_PP_VALIDATED defined in [BR-DBMSPP] require a more restrictive operational environment. In particular, the operational environment required by these assumptions is part of the TOE.
- A.PHYSICAL defined in [BR-DBMSPP] is similar to A.PROTECT and A.LOCATE.
- The rest of the personnel, procedural and connectivity assumptions defined in [ZOSST] and [CAPP] do not conflict with the assumptions in [BR-DBMSPP] mentioned above.

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

The following table lists the security objectives defined in [BR-DBMSPP], [CAPP] and [ZOSST], all of which are applicable to the security problem definition:

Name	Defined in	Comment
O.AUTHORIZATION	[ZOSST] copied from [CAPP]	
O.DISCRETIONARY_ACCESS	[ZOSST] copied from [CAPP]	
O.MANDATORY_ACCESS (Labeled Security Mode only)	[ZOSST]	
O.AUDITING called O.AUDIT_GENERATION in [BR-DBMSPP]	[BR-DBMSPP] and [ZOSST] copied from [CAPP]	Nearly the same phrasing; O.AUDITING additionally requires that the TSF must present the information to authorized administrators
O.RESIDUAL_INFORMATION	[BR-DBMSPP] and [ZOSST] copied from [CAPP]	
O.MANAGE	[BR-DBMSPP] and [ZOSST] copied from [CAPP]	Nearly the same phrasing; [BR-DBMSPP] additionally requires that the TOE restrict functions and facilities from unauthorized use.
O.ENFORCEMENT	[ZOSST] copied from [CAPP]	
O.COMPROT	[ZOSST]	
O.ACCESS_HISTORY	[BR-DBMSPP]	
O.ADMIN_GUIDANCE	[BR-DBMSPP]	
O.ADMIN_ROLE	[BR-DBMSPP]	
O.AUDIT_GENERATION	[BR-DBMSPP]	
O.CONFIGURATION_IDENTIFICATION	[BR-DBMSPP]	
O.DOCUMENTED_DESIGN	[BR-DBMSPP]	
O.INTERNAL_TOE_DOMAINS	[BR-DBMSPP]	
O.MEDIATE	[BR-DBMSPP]	
O.PARTIAL_FUNCTIONAL_TEST	[BR-DBMSPP]	
O.PARTIAL_SELF_PROTECTION	[BR-DBMSPP]	
O.TOE_ACCESS	[BR-DBMSPP]	supplemented and refined by O.AUTHORIZATION, O.DISCRETIONARY_ACCESS and O.MANDATORY_ACCESS
O.VULNERABILITY_ANALYSIS	[BR-DBMSPP]	

Table 4: Security objectives for the TOE

No additional objective for the TOE is defined by this ST.

4.2 Security objectives for the operational environment

The following table lists the security objectives for the operational environment of the [BR-DBMSPP], [CAPP], and [ZOSST].

Name	Defined in	Comment
OE.INSTALL	[ZOSST] copied from [CAPP]	
OE.PHYSICAL_zOS	[ZOSST] copied from [CAPP]	
OE.CREDEN	[ZOSST] copied from [CAPP]	
OE.HW_SEP	[ZOSST]	
OE.HW_CRYPTO	[ZOSST]	
OE.CLASSIFICATION (Labeled Security Mode only)	[ZOSST]	
OE.NO_EVIL	[BR-DBMSPP]	
OE.NO_GENERAL_PURPOSE	[BR-DBMSPP]	
OE.OS_PP_VALIDATED	[BR-DBMSPP]	
OE.PHYSICAL_DBMS	[BR-DBMSPP]	

Table 5: Security objectives for the operational environment defined in [BR-DBMSPP], [CAPP] and [ZOSST]

No additional objective for the operational environment is defined by this ST.

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 by the security objectives and security problems defined in [ZOSST] (using [CAPP]) and [BR-DBMSPP]. The rationales for the security objectives and security problem definition provided in these documents are also applicable to this ST and therefore not repeated here.

The security objectives for the TOE included in table 6, which have been drawn from [BR-DBMSPP], have not been traced back by at least one security functional requirement; instead, they were covered by security assurance requirements. This coverage is not allowed in CC 3.1; this is a known inconsistency in [BR-DBMSPP] when adapted from CC 2.3 to CC 3.1

However, an analysis of the security problem definition draws to the conclusion that these security objectives are aimed at covering threats that may occur in the development process. It is reasonable then to expect that security assurance requirements satisfy these security objectives.

As this security target claims a higher EAL than the EAL expected in [BR-DBMSPP], the table below indicates the security assurance component that correspond to the EAL claimed in this ST.

Security Objective	Security Assurance Component
O.ADMIN_GUIDANCE	AGD_PRE.1, AGD_OPE.1
O.CONFIGURATION_IDENTIFICATION	ALC_CMS.4, ALC_FLR.3
O.DOCUMENTED_DESIGN	ADV_FSP.4, ADV_TDS.3
O.INTERNAL_TOE_DOMAINS	ADV_ARC.1
O.PARTIAL_FUNCTIONAL_TEST	ATE_COV.2, ATE_FUN.1, ATE_IND.2
O.PARTIAL_SELF_PROTECTION	ADV_ARC.1
O.VULNERABILITY_ANALYSIS	AVA_VAN.3

Table 6- [BR- DBMSPP] coverage for security objectives

4.4 Rationale for Demonstrable Conformance

The following sections provides the rationale to justify that the security objectives for the TOE and the security objectives for the operational environment defined in this ST are more restrictive than the security objectives defined in each protection profile claimed.

4.4.1 Security Objectives for the TOE

As described in section 4.1, all security objectives provided in [CAPP] and [BR-DBMSPP] are included in this ST, only the security objectives O.MANDATORY_ACCESS and O.COMPROT are incorporated in [ZOSST]. O.MANDATORY_ACCESS is reproduced here to cover the Labeled Security mode in which the TOE can be set, both in z/OS and DB2 and O.COMPROT is reproduced to cover the Inter-TSF trusted channel functionality of the TOE.

The security objectives for the TOE defined in this ST are more restrictive than the set included in [CAPP] and [BR-DBMSPP] because:

- O.ADMIN_GUIDANCE, O.CONFIGURATION_IDENTIFICATION, O.DOCUMENTED_DESIGN, O.PARTIAL_FUNCTIONAL_TEST and O.VULNERABILITY_ANALYSIS defined in [BR-DBMSPP] are only objectives related to activities that are part of the software development life cycle, which are covered by security assurance requirements at a level commensurate with the EAL required in [CAPP] and the EAL claimed in this ST. Therefore, these security objectives provide similar coverage in both protection profiles.
- O.MEDIATE defined in [BR_DBMSPP] requires the protection of user data in accordance with the security policy; this security objective has a similar meaning of O.ENFORCEMENT defined in [CAPP], which requires the TSF to ensure that organization security policies are properly enforced. Therefore, both security objectives provide the same level of coverage on both protection profiles.
- O.INTERNAL_TOE_DOMAINS and O.PARTIAL_SELF_PROTECTION defined in [BR-DBMSPP] require the existence of internal domains for separation of information belonging to concurrent users and the protection of the TOE and its resources from external interference; these security objectives are connected with the need of a security architecture. Although more

general, O.ENFORCEMENT defined in [CAPP] also aims at this direction. In CC 3.1 this is covered by the ADV_ARC.1 component, which is required in both protection profiles. Therefore, these security objectives provide similar coverage in both protection profiles.

- O.AUDITING in [CAPP] and O.AUDIT_GENERATION in [BR-DBMSPP] exist in both protection profiles and are similar in meaning. O.AUDITING was selected for this ST as it is more restrictive; requiring that the TSF must present the information to authorized administrators.
- O.RESIDUAL_INFORMATION is defined in both protection profiles with the same meaning.
- O.MANAGE is defined in both protection profiles with the same meaning.
- O.ADMIN_ROLE defined in [BR-DBMSPP] requires the existence of authorized administrator roles; this objective is implicitly included in O.MANAGE defined in [CAPP].
- O.TOE_ACCESS defined in [BR-DBMSPP] is refined in more detail by O.AUTHORIZATION and O.DISCRETIONARY_ACCESS (defined in [CAPP]) and O.MANDATORY_ACCESS (defined in this ST and also in [ZOSST]), therefore the four security objectives together contribute to a more restrictive ST.
- O.ACCESS_HISTORY defined in [BR-DBMSPP] implies additional requirements for storing and retrieving information related to previous attempts to establish sessions; it does not collide with any other security objective defined in this ST.
- O.MANDATORY_ACCESS defined in [ZOSST] implies additional requirements to the TSF for the enforcing of a Mandatory Access Policy when the TOE is in Labeled Security Mode. This security objective is supplemental to O.DISCRETIONARY_ACCESS in the sense that only the DAC policy can be enforced or the DAC policy in combination with the MAC policy. Therefore, O.MANDATORY_ACCESS provides a more restrictive ST in the situation where the TOE is in Labeled Security Mode.
- O.COMPROT defined in [ZOSST] implies additional requirements to the TSF for establishing a trusted channel between the TOE and another trusted IT product; it does not collide with any other security objective defined in this ST.

4.4.2 Security Objectives for the Operational Environment

As described in section 4.2, all security objectives for the operational environment provided in [CAPP] and [BR-DBMSPP] are included in this ST; there are also new security objectives defined in [ZOSST] that are specifically related with Label Security mode and the hardware platform required by the z/OS underlying platform.

The security objectives for the operational environment defined in this ST are more restrictive than the set included in [CAPP] and [BR-DBMSPP] because:

- OE.PHYSICAL_zOS defined in [CAPP] and OE.PHYSICAL.DBMS defined in [BR-DBMSPP] (renamed as in both protection profiles are named OE.PHYSICAL) provide similar physical protection to IT assets, the TOE itself and the stored processed and transmitted information.
- OE.HW_SEP and OE.HW_CRYPTO are defined in [ZOSST] and required by the z/OS underlying platform; they provide specific requirements apart from OE.OS_PP_VALIDATED defined in [BR-DBMSPP] for the database underlying platform.
- OE_INSTALL, defined in [CAPP], OE.NO_EVIL defined in [BR-DBMSPP] and OE.CLASSIFICATION (defined also in [ZOSST] for Labeled Security mode) defines objectives related with organizational policies that provide a more restrictive operational environment.
- OE.OS_PP_VALIDATED is specifically defined in [BR-DBMSPP] for a more restrictive underlying platform, which must be validated against an NSA sponsored OS PP of at least Basic Robustness. Additionally OE.NO_GENERAL_PURPOSE, defined in the same protection profile, restricts the usage of the underlying platform exclusively for the database.

5 Extended components definition

This ST does not define extended components; only extensions defined in [CAPP] and [BR-DBMSPP] are used.

6 Security requirements

6.1 TOE security functional requirements

This chapter defines the functional requirements for the TOE. Functional requirement components in this Security Target were drawn from the Controlled Access Protection Profile ([CAPP]), the U.S. Government Protection Profile for Database Management Systems in Basic Robust Environments ([BR-DBMSPP]) and 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.

As [CAPP] and [BR-DBMSPP] define a different convention for the operations performed in the protection profile, this ST adopts the same convention used in [ZOSST] for both protection profiles: all operations already performed in [CAPP] and [BR-DBMSPP] are shown in bold and italics.

Refinement, assignment and selection operations performed in this Security Target on security functional components are marked in underlined text, so as to be able to overlap the operations already performed in the protection profiles.

This Security Target defines security functional requirements that exist both in [CAPP] and [BR-DBMSPP]. In this case, the text in the final SFR is merged, taking precedence the most complete and restrictive security functional component. The text not common is shown in underlined text. It is considered a refinement operation as the result of merging both source SFRs.

Some SFRs defined in the protection profiles have been refined to reflect changes in Revision 3 of CC 3.1.

The SFRs id is also renamed using the following rules:

- When the SFR already exists in [ZOSST] and needs to be iterated to provide additional requirements for [CAPP], the security functional component is iterated with the suffix "DB2" between parentheses. In case the component is also defined in [BR-DBMSPP], then a note is provided at the end of the SFR to declare the original component id defined in [BR-DBMSPP] that the iteration covers.
- When the SFR is defined in [BR-DBMSPP] and it is not defined in [ZOSST], the component id provided in [BR-DBMSPP] remains.
- When the SFR is defined in both [BR-DBMSPP] and [ZOSST] and the SFRs represent different semantics, then the component id defined in [BR-DBMSPP] is renamed with the suffix "DB2" within parenthesis (as if it was an iteration).
- When the SFR is defined in both [BR-DBMSPP] and [ZOSST] and the SFRs represent similar semantics, the more restrictive component is used, marking the differences in both texts with normal underlined font.

SFRs are marked "Labeled Security Mode only" if they are only applicable in the Labeled Security mode of operation. All other SFRs (or portions thereof) not marked as "Labeled Security Mode only" are applicable in both Labeled Security and CAPP mode. Application notes marked "from CAPP" have been copied from this protection profile.

To support a better understanding of the combination Security Target of the z/OS platform [ZOSST] vs. this DB2 Security Target, **Table 7** below lists the Security Functional Requirements for the z/OS platform. The SFRs for DB2 defined in this Security Target are listed afterwards.

Name	Title
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association

Name	Title
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.1	Guarantees of audit data availability
FAU_STG.3	Action in case of possible audit data loss
FAU_STG.4	Prevention of audit data loss
FCS_CKM.1(1)	Cryptographic key generation (TLS/SSL: symmetric algorithms)
FCS_CKM.1(2)	Cryptographic key generation (IPSec: symmetric algorithms)
FCS_CKM.1(3)	Cryptographic key generation (SSH: symmetric algorithms)
FCS_CKM.1(4)	Cryptographic key generation (z/OS Network Authentication Service: symmetric algorithms)
FCS_CKM.1(5)	Cryptographic key generation (public/private Keys)
FCS_CKM.1(6)	Cryptographic key generation (SSH: host public/private keys)
FCS_CKM.2(1)	Cryptographic key distribution (RSA and DSA public keys)
FCS_CKM.2(2)	Cryptographic key distribution (TLS/SSL: symmetric keys)
FCS_CKM.2(3)	Cryptographic key distribution (IPSec: Diffie-Hellman key exchange for symmetric session keys)
FCS_CKM.2(4)	Cryptographic key distribution (SSH: Diffie-Hellman key exchange for symmetric session keys)
FCS_CKM.2(5)	Cryptographic key distribution (z/OS Network Authentication Service: session keys)
FCS_COP.1(1)	Cryptographic operation (TLS/SSL: RSA and DSA signatures)
FCS_COP.1(2)	Cryptographic operation (TLS/SSL: symmetric operations)
FCS_COP.1(3)	Cryptographic operation (IPSec: payload encryption)
FCS_COP.1(4)	Cryptographic operation (IPSec: HMAC-SHA)
FCS_COP.1(5)	Cryptographic operation (SSH: symmetric operations)
FCS_COP.1(6)	Cryptographic operation (z/OS Network Authentication Service: symmetric operations)
FDP_ACC.1	Discretionary access control policy
FDP_ACF.1(1)	Discretionary access control functions for non-LDAP, non-z/OS UNIX objects
FDP_ACF.1(2)	Discretionary access control functions for z/OS UNIX objects
FDP_ACF.1(3)	Discretionary access control functions for LDAP LDBM objects
FDP_ETC.1	Export of unlabeled user data (Label Security Mode only)
FDP_ETC.2	Export of labeled user data (Label Security Mode only)
FDP_IFC.1	Mandatory access control policy (Label Security Mode only)
FDP_IFF.2	Mandatory access control functions (Label Security Mode only)
FDP_ITC.1	Import of unlabeled user data (Label Security Mode only)
FDP_ITC.2	Import of labeled user data (Label Security Mode only)
FDP_RIP.2	Object residual information protection
NOTE 1	Subject residual information protection
FDP_UCT.1	Basic data exchange confidentiality
FDP_UIT.1	Data exchange integrity
FIA_ATD.1	User attribute definition
FIA_SOS.1	Strength of authentication data
FIA_UAU.1	Authentication

Name	Title
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.7	Protected authentication feedback
FIA_UID.1	Identification
FIA_USB.1	User-subject binding
FMT_MSA.1(1)	Management of object security attributes
FMT_MSA.1(2)	Management of object security attributes for MAC (Label Security Mode only)
FMT_MSA.2	Secure security attributes
FMT_MSA.3(1)	Static attribute initialization
FMT_MSA.3(2)	Static attribute initialization for MAC (Label Security Mode only)
FMT_MTD.1(1)	Management of the audit trail
FMT_MTD.1(2)	Management of audited events
FMT_MTD.1(3)	Management of user attributes
FMT_MTD.1(4)	Management of authentication data
FMT_MTD.1(5)	Management of cryptographic keys
FMT_MTD.1(6)	Management of digital certificates
FMT_MTD.1(7)	Management of IPSEC, IP Filtering, and Defensive Filtering configuration from the command line
FMT_MTD.1(8)	Management of IPSEC network configuration via network interfaces
FMT_MTD.1(9)	Management of additional TOE configuration data
FMT_REV.1(1)	Revocation of user attributes
FMT_REV.1(2)	Revocation of object attributes
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security management roles
FPT_STM.1	Reliable time stamps
FPT_TDC.1	Inter-TSF basic TSF data consistency (Label Security Mode only)
FTP_ITC.1	Inter-TSF trusted channel

Table 7: Security Functional Requirements for the z/OS platform

The requirements above have already been stated in the z/OS ST [ZOSST] and are fulfilled by the z/OS platform, if not indicated otherwise in **Table 8**.

Table 8 below lists the Security Functional Requirement (SFR) defined in this Security Target. Each row describes the SFR, where it was originally defined ([CAPP], [DBMS-PP], [ZOSST] or CC Part 2) and whether the functionality is enforced by DB2 or the underlying z/OS platform. As the z/OS security target is used in combination of this Security Target, please notice that those SFRs marked as defined in [ZOSST] are not duplicated in the SFR section of thi ST. See [ZOSST] for the definition of those SFRs.

Name	Title	Defined by				Enforced by	
		CAPP	BR-DBMSPP	CC Part 2	z/OS ST	z/OS	DB2
FAU_GEN.1(DB2)	Audit data generation	✓	✓				✓
FAU_GEN_(EXT).2	User identity association	✓	✓			✓	
FAU_SEL.1(DB2)	Selective audit	✓	✓			✓	
FDP_ACC.1(DB2)	Discretionary access control policy in DB2	✓	✓				✓
FDP_ACF.1(DB2)	Discretionary access control functions for DB2 objects	✓	✓				✓
FDP_ETC.1	Export of unlabeled user data (Labeled Security Mode only)				✓		✓
FDP_ETC.2	Export of labeled user data (Labeled Security Mode only)				✓		✓
FDP_IFC.1(DB2)	Mandatory access control policy in DB2 (Labeled Security Mode only)			✓			✓
FDP_IFF.2	Mandatory access control functions (Labeled Security Mode only)				✓		✓
FDP_ITC.1	Import of unlabeled user data (Labeled Security Mode only)				✓		✓
FDP_ITC.2	Import of labeled user data (Labeled Security Mode only)				✓		✓
FDP_RIP.2	Object/Subset residual information protection	✓	✓			✓	✓
FDP_UCT.1	Basic data exchange confidentiality				✓	✓	
FDP_UIT.1	Data exchange integrity				✓	✓	
FIA_ATD.1(DB2)	User attribute definition	✓	✓				✓
FIA_UAU.1(DB2)	Authentication	✓					✓
FIA_UID.1(DB2)	Identification	✓					✓
FIA_USB.1(DB2)	User-subject binding	✓					✓
FMT_MOF.1	Management of security functions behavior		✓				✓
FMT_MSA.1(DB2-1)	Management of security attributes in DB2	✓	✓			✓	
FMT_MSA.1(DB2-2)	Management of object security attributes for DB2 rows (Labeled Security Mode only)			✓			✓
FMT_MSA_(EXT).3	Static attribute initialization in DB2	✓	✓				✓
FMT_MSA.3(DB2-2)	Static attribute initialization for rows in DB2 tables and MAC (Labeled Security Mode only)			✓			✓
FMT_MTD.1(DB2)	Management of TSF data		✓				✓
FMT_REV.1(1)	Revocation of user attributes	✓	✓			✓	
FMT_REV.1(2)	Revocation of object attributes	✓	✓			✓	✓
FMT_SMF.1(DB2)	Specification of management functions	✓	✓				✓
FMT_SMR.1(DB2)	Security management roles	✓	✓				✓
FPT_TDC.1(DB2)	Inter-TSF basic TSF data consistency (Labeled Security Mode only)			✓			✓
FPT_TRC_(EXT).1	Internal TSF consistency		✓				✓
FTA_MCS.1	Basic limitation on multiple concurrent sessions		✓			✓	

Name	Title	Defined by				Enforced by	
		CAPP	BR-DBMSPP	CC Part 2	z/OS ST	z/OS	DB2
FTA_TAH_(EXT).1	TOE access history		✓			✓	
FTA_TSE.1	TOE session establishment		✓				✓

Table 8: Security Functional Requirements in DB2

The following functional requirements already defined in [ZOSST] are supplemented with application notes to explain the implementation within DB2 and are not duplicated in this ST:

SFR	Application Notes
FDP_ETC.2	Within DB2 the labels of rows in a table are stored in a dedicated column defined with AS SECURITY LABEL. When the table or the whole database is exported, the labels of the rows are exported as part of the table or database.
FDP_UCT.1	Note that this requirement applies for connections using the protocols mentioned. Other connections (including DRDA connections to DB2) are not protected by the TOE and therefore need to be protected by the TOE environment if such a protection is required. Note that FDP_UCT.1 is defined in [ZOSST]. Since there “user data” is meant with “object” (see O.COMPROT: [...] establishing a trusted channel between the TOE and another trusted IT product that protect the user data transferred over this channel [...]) the SFR based on CC 2.3 can be replaced by the one of CC 3.1. Since the [ZOSST] is already certified this is accepted for this ST, too.
FDP_UIT.1	Note that this requirement applies for connections using the protocols mentioned. Other connections (including DRDA connections to DB2) are not protected by the TOE and therefore need to be protected by the TOE environment if such a protection is required.
FMT_MSA.1(1)	Since access to all DB2 objects in the evaluated configuration is controlled by RACF, the rules for the management of the object security attributes for DB2 objects are identical to those for non-UNIX, non-LDAP z/OS objects.
FMT_MSA.3(1)	Since the access control for DB2 objects in the evaluated configuration is performed by RACF, the general rules for the attribute initialization defined by RACF apply.

Table 9: DB2 Application Notes for SFRs

SFR	CAPP ¹					BR-DBMSPP					z/OS ST	CC Part 2					Comments
	D	A	S	R	I	D	A	S	R	I		D	A	S	R	I	
FAU_GEN.1(DB2)	✓			✓	✓	✓		✓	✓							FAU_GEN.1-NIAP-0410 in [BR-DBMSPP]	
FAU_GEN_(EXT).2	✓					✓										Defined as FAU_GEN.2 in CAPP.	
FAU_SEL.1(DB2)	✓			✓	✓	✓	✓	✓								FAU_SEL.1-NIAP-0407 in [BR-DBMSPP]	
FDP_ACC.1(DB2)	✓	✓			✓	✓			✓								
FDP_ACF.1(DB2)	✓	✓		✓	✓	✓			✓							FDP_ACF.1-NIAP-0407 in [BR-DBMSPP]	
FDP_ETC.1											✓						
FDP_ETC.2											✓					Added application note	
FDP_IFC.1(DB2)												✓	✓			✓	
FDP_IFF.2											✓						
FDP_ITC.1											✓						
FDP_ITC.2											✓						
FDP_RIP.2	✓			✓	✓	✓						✓			✓	Supersedes FDP_RIP.1 defined in [BR-DBMSPP]	
FDP_UCT.1											✓					Added application note	
FDP_UIT.1											✓					Added application note	
FIA_ATD.1(DB2)	✓	✓		✓	✓	✓	✓		✓								
FIA_UAU.1(DB2)	✓	✓			✓												
FIA_UID.1(DB2)	✓	✓			✓												
FIA_USB.1(DB2)	✓	✓			✓												
FMT_MOF.1						✓											
FMT_MSA.1(DB2-1)	✓	✓		✓	✓	✓	✓			✓							
FMT_MSA.1(DB2-2)												✓	✓		✓	✓	
FMT_MSA_(EXT).3	✓				✓	✓			✓							FMT_MSA_(EXT).3	
FMT_MSA.3(DB2-2)												✓	✓		✓	✓	
FMT_MTD.1(DB2)						✓											
FMT_REV.1(1)	✓	✓				✓	✓										
FMT_REV.1(2)	✓	✓		✓		✓	✓		✓								
FMT_SMF.1(DB2)						✓	✓										
FMT_SMR.1(DB2)	✓	✓		✓	✓	✓	✓		✓								
FPT_TDC.1(DB2)												✓	✓				
FPT_TRC_(EXT).1						✓											
FTA_MCS.1						✓		✓									
FTA_TAH_(EXT).1						✓											
FTA_TSE.1						✓	✓										
FTP_ITC.1												✓					

¹ **References:** (D)efined in PP or CC Part 2, (A)ssignment, (S)election, (R)efinement, (I)teration

Table 10 - Operations performed in SFRs

6.1.1 Security audit (FAU)

6.1.1.1 Audit data generation (FAU_GEN.1(DB2))

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 **DB2** audit functions;
- b) All auditable events for the **basic** level of audit listed in **Table 11: DB2 auditable events: this includes all auditable events except FIA UID.1's user identity during failures:**
- 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**

Application Note 1: FAU_GEN.1(DB2) refines FAU_GEN.1-NIAP-0410 defined in [BR-DBMSPP] and FAU_GEN.1 defined in [CAPP], notice that only refinement operations on the functional component defined in [BR-DBMSPP] are shown.

Application Note 2: The level of audit is raised to basic in order to comply with FAU_GEN.1 defined in [CAPP]. Additionally, **Table 11** includes audit events provided by DB2 not captured by z/OS in [ZOSST], audit events required by [BR-DBMSPP].and audit events from new SFRs derived from CC Part 2.

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 the outcome (success or failure) of the event; **and**
- b) **(Labeled Security Mode only) The sensitivity labels of subjects, objects, or information involved; and**
- c) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **information specified in column three "Details" of Table 11: DB2 auditable events**

Security Functional Requirement	Auditable Event(s)	Details
FAU_GEN.1(DB2)	Startup and shutdown of the DB2 audit functions.	SMF record type 102 (DB2). DB2 IFCID 0004 and 0005. DSN1SMFP can be used to report on these records.
FAU_GEN_(EXT).2	None.	
FAU_SEL.1(DB2)	All modifications to the audit configuration that occur while the audit collection functions are operating.	DB2 audit trace audit class 3. SMF record type 102, IFCID 0142, IFCID 0106. DSN1SMFP can be used to report on these records. The identity of the authorized administrator that made the change to the audit configuration.
FDP_ACC.1(DB2)	None.	

Security Functional Requirement	Auditable Event(s)	Details
FDP_ACF.1(DB2)	All requests to perform an operation on an object covered by the Security Function Policy (SFP).	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. The identity of the subject performing the operation.
FDP_ETC.1 (Labeled Security mode)	All attempts to export information.	SMF type 80 record, event code 2, for TAPEVOL class. (see Note 1)
FDP_ETC.2 (Labeled Security mode)	All attempts to export information.	SMF type 80 record, event code 2, for TAPEVOL class. (see Note 2)
FDP_ETC.2 (Labeled Security mode)	Overriding of human-readable output marking. (Additional)	SMF type 80 record, event code 2, for PSFMPL class. Covered by z/OS/RACF.
FDP_IFC.1(DB2) (Labeled Security mode)	None.	
FDP_IFF.2 (Labeled Security mode)	All decisions on requests for information flow.	SMF type 80 record, event code 2, with reason indicating SECLABEL AUDIT
FDP_ITC.1 (Labeled Security mode)	All attempts to import user data, including any security attributes.	SMF type 80 record, event code 2, associated with TAPEVOL profiles.
FDP_ITC.2 (Labeled Security mode)	All attempts to import user data, including any security attributes.	SMF type 80, event code 2, associated with TAPEVOL profiles.
FDP_RIP.2	None.	
FIA_ATD.1(DB2)	None.	
FIA_UAU.1(DB2)	All use of the authentication mechanism.	SMF type 80 record, event code 1, various qualifiers and SMF record type 30 subtypes 1 and 5. Also SMF type 80, event code 68, qualifier 0 (success) or 1 (failure) to generate a Kerberos TGT. Also SMF type 83, subtype 3, event codes 2,4,6,11 for LDAP bind operations. Covered by z/OS/RACF. In the case of a user authentication using DRDA, RACF is called for authentication. (see Note 3)
FIA_UID.1(DB2)	All use of the user identification mechanism, including the identity provided <i>during successful attempts</i> .	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. (see Note 3)
FIA_USB.1(DB2)	Success and failure of binding user security attributes to a subject (e.g. success and failure to create a subject).	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. (see Note 3)
FMT_MOF.1	None	

Security Functional Requirement	Auditable Event(s)	Details
FMT_MSA.1(DB2-1)	Modifications of the default setting of permissive or restrictive rules. All modifications of the initial value of security attributes.	SMF type 80 record (generated by the RACF commands). Covered by z/OS/RACF.
FMT_MSA.1(DB2-2)	All modifications of the values of security attributes.	DB2 audit class 4 IFCID 0143 (row values can be found in the DB2 log). DSN1SMFP can be used to report on these records.
FMT_MSA_(EXT).3	None	
FMT_MSA.3(DB2-2)	Modifications of the default setting of permissive or restrictive rules. All modifications of the initial value of security attributes.	SMF type 80 record (generated by the RACF commands).
FMT_MTD.1(DB2)	All modifications to the values of TSF data.	SMF type 80 record (generated by the RACF commands). Covered by z/OS/RACF.
FMT_REV.1(1)	All attempts to revoke security attributes.	SMF type 80 record (generated by the RACF commands). Identity of individual attempting to revoke security attributes. Covered by z/OS/RACF.
FMT_REV.1(2)	All modifications to the values of TSF data.	SMF type 80 record (generated by the RACF commands). Identity of individual attempting to revoke security attributes. Covered by z/OS/RACF.
FMT_SMF.1(DB2)	None specifically associated with this SFR, but auditing is covered under the FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_REV.1, FAU_SAR.1, FAU_SEL.1, FAU_STG.3, FAU_STG.4, and FMT_SMR.1 requirements which are implied by FMT_SMF.1 as discussed in chapter 8.	Identity of the administrator performing these functions.
FMT_SMR.1(DB2)	Modifications to the group of users that are part of a role.	SMF type 80 record (generated by the RACF commands that manage DB2 profiles defining the privileges of the DB2 user roles). Identity of authorized administrator modifying the role definition. Covered by z/OS/RACF. (See Note 4)
FMT_SMR.1(DB2)	Every use of the rights of a role. (Additional / Detailed)	SMF type 80 record. Covered by z/OS/RACF.
FPT_TDC.1(DB2)	None	
FPT_TRC_(EXT).1	Restoring consistency	
FTA_MCS.1	Rejection of a new session based on the limitation of multiple concurrent sessions.	SMF record type 102, IFCID 83 with QW0083AD flag
FTA_TAH_(EXT).1	None.	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism	Identity of the individual attempt to establish a session.

Table 11: DB2 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. DB2 does not generate additional audit records for exporting data, but relies on the audit functions of z/OS when exporting unlabeled data. This includes the export to a printer, where z/OS controls printers capable to print data at different security levels. Data from DB2 is handled in this case like data from any other application.
- Note 2:** Exporting labeled data is performed by unloading data from the database to one or more BSAM sequential data sets and those can be copied to a tape for export. Tables with row-level security can be unloaded and the BSAM data sets will then contain the security labels. The BSAM data sets are created by enforcing the mandatory access control, i.e. they will have a security label that dominates the security label of every row that has been unloaded. When the data sets are written to tapes, z/OS audits this action.
- Note 3:** 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 4:** The DB2 user 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 User and/or group identity association (FAU_GEN_(EXT).2)

FAU_GEN_(EXT).2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Application Note 1: This functional requirement is fulfilled by z/OS and covered by FAU_GEN.2 defined in [ZOSST]; it is included in this ST for completeness with the set of SFRs defined in [BR-DBMSPP]. Notice that the modification included in this extended functional component defined in [BR-DBMSPP] is also addressed in the application note of FAU_GEN.2 in [CAPP], therefore both components are similar in meaning.

Application Note 2: Audit events in DB2 and z/OS can be identified by user identity but not by group identity; therefore, this part of the requirement defined in [BR-DBMSPP] is not included.

Application Note 3: The extended component defined in [BR-DBMSPP] does not include the list of dependencies, management or audit activities. As changes compared with FAU_GEN.2 are minimal, the ST author assumes that the definition in CC part 2 is still applicable.

6.1.1.3 Selective audit (FAU_SEL.1(DB2))

FAU_SEL.1.1 The TSF shall ***allow only the administrator*** to select the set of events to be audited from the set of all auditable events based on the following attributes:

- a) ***user identity;***
- b) ***event type;***
- c) ***object identity (object type and object name);***
- d) ***subject identity;***
- e) ***success of auditable security events;***
- f) ***failure of auditable security events; and***
- g) ***subject sensitivity label; (Labeled Security Mode only)***
- h) ***object sensitivity label; (Labeled Security Mode only)***

Application note 1: The requirement can be satisfied for the SMF records generated by RACF and this should be sufficient (since it is not required that **all** auditable events are covered by this requirement, the DB2 audit trace does not necessarily need to be configurable as required by FAU_SEL.1).

Application note 2: This functional requirement covers FAU_SEL.1-NIAP-0407 defined in [BR-DBMSPP] and FAU_SEL.1 defined in [CAPP].

Application note 3: Audit events in DB2 and z/OS can be included or excluded by user identity but not by group identity; therefore, this part of the requirement defined in [BR-DBMSPP] is not included.

6.1.2 User data protection (FDP)

6.1.2.1 Discretionary access control policy in DB2 (FDP_ACC.1(DB2))

FDP_ACC.1.1 The TSF shall enforce the ***Discretionary Access Control policy*** on ***DB2 subjects (requests coming from allied address spaces or external DRDA clients) acting on behalf of users, DB2 objects (databases, table spaces, tables, columns, views, storage groups, buffer pools, plans, collections, packages, database roles, schemas, sequences, indexes, stored procedures and trusted contexts) and all operations among subjects and objects covered by the DAC policy.***

Application Note: This functional requirement iterates FDP_ACC.1 defined in [CAPP] and also covers FDP_ACC.1 defined in [BR-DBMSPP].

6.1.2.2 Discretionary access control functions for DB2 Objects (FDP_ACF.1(DB2))

FDP_ACF.1.1 The TSF shall enforce the ***Discretionary Access Control policy*** to ***DB2*** objects based on the following:

- a) ***The DB2 user identity and group membership(s) associated with a DB2 subject; and***
- b) ***The following access control attributes associated with an object:***
 - ***The primary authorization ID of the user***

- The user's access right in the RACF access control list for the RACF profile protecting the DB2 privilege the user is using to access the object
- The DB2 role(s) of the user
- The ownership of the DB2 object

Application note: This functional requirement iterates FDP_ACF.1 defined in [CAPP] and also covers FDP_ACF-NIAP-0407 defined in [BR-DBMSPP].

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 Mandatory Access Control (Labeled Security Mode) must allow access and the following algorithm for the Discretionary Access Control must also result in granting access and the user has access to a DB2 authority for a DB2 object if

- the authority is granted by the implicit rights of a user role and the user has that role
or
- the TOE is not in Labeled Security Mode and the user is the owner of the DB2 object and the requested DB2 authority is granted to the owner of the object
or
- the TOE is not in Labeled Security Mode, the user has established a trusted connection with a database role assigned, the database role is the owner of the DB2 object and the requested DB2 authority is granted to the owner of the object
or
- if the user is granted sufficient access by the following algorithm:
 1. If the user (as defined by the primary authorization ID) has sufficient access authority in the standard access list of the RACF profile protecting the requested authority to the DB2 object, access is granted.
 2. If the current group of the user has sufficient authority in the standard access list of the RACF profile protecting the requested authority to the DB2 object, access is granted.
 3. 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 the requested authority to the DB2 object, access is granted.
 4. If a user ID of * is found on the standard access list with sufficient access authority, the current user is defined to RACF without the RESTRICTED attribute, access is granted.
 5. If the universal access authority (UACC) for the resource provides sufficient access authority and the requesting user is not defined with the RESTRICTED attribute, access is granted.
 6. 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.

7. **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). 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.**
 - 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, access is granted.**
8. **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.**
9. **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.**
10. **If none of those conditions has granted access, access is denied.**

Application note 1: In the above algorithm, sufficient access that a user requires to pass a discretionary access check for a DB2 resource depends on whether the RACF MLS option is active:

- If the RACF MLS option is not active, a user with at least READ authorization to the resource has sufficient access.
- If the RACF MLS option is active and the request is not a write request, a user with at least READ authorization to the resource has sufficient access.
- If the RACF MLS option is active, and the request involves a write request, a user with at least UPDATE authorization to the resource has sufficient access.

Application note 2: The terminology used in the rules described above corresponds to z/OS and RACF, which differ a bit from the one used in DB2:

- User roles for security management are known in DB2 as Administrative Authorities. Each administrative authority possesses 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).
- The term "authority" is used as a synonym of the concept of privilege in DB2. 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.

- 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 connection.

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 (unless the CSA or PRIVATE operand was specified on the authorization request).**
- b) If the user has the PRIVILEGED attribute, RACF grants the request (unless the CSA or PRIVATE operand was specified on the authorization request).**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **following rules: none.**

6.1.2.3 Mandatory access control policy in DB2 (FDP_IFC.1(DB2)) (Labeled Security Mode only)

FDP_IFC.1.1 The TSF shall enforce the **Mandatory Access Control policy on DB2 processes acting on behalf of users, and rows in tables of DB2 databases, and all operations among subjects and objects covered by the MAC policy.**

6.1.2.4 Subset residual information protection (FDP_RIP.2)

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **allocation of the resource to** all **DB2** objects.

Application note: this SFR supersedes FDP_RIP.1 defined in [BR-DBMSPP].

6.1.3 Identification and authentication (FIA)

6.1.3.1 User attribute definition in DB2 (FIA_ATD.1(DB2))

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- Database user identifier and/or group memberships;**
- Security-relevant user roles; and**
- authentication data;**
- user clearances; (in Labeled Security Mode)**

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 connections) and the concept of user role defined in CC. This

difference is further explained in FMT_SMR.1.

Application note 2: User roles are not stored in the user profile but are defined by access rights to RACF profiles related to the role. This is seen as an implementation specific detail and for the view of this Security Target the roles are defined as user attributes.

6.1.3.2 Authentication *in DB2* (FIA_UAU.1(DB2))

FIA_UAU.1.1 The TSF shall allow *no request to DB2* 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 Identification *in DB2* (FIA_UID.1(DB2))

FIA_UID.1.1 The TSF shall allow *no request to DB2* 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 User-subject binding (FIA_USB.1(DB2))

FIA_USB.1.1 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) used to enforce the Discretionary Access Control policy;*
- c) *The group membership or memberships used to enforce the Discretionary Access Control policy;*
- d) *In Labeled Security Mode: The sensitivity label used to enforce the Mandatory Access Control policy, which consists of the following:*
 - *A hierarchical level; and*
 - *A set of non-hierarchical categories.*
- e) *The DB2 primary authorization ID*
- f) *The DB2 user roles SYSADM, Install SYSADM, SYSCTRL, SYSOPR, Install SYSOPR, DBADM, DBCTRL, DBMAINT.*
- g) *In a trusted connection, 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).*

FIA_USB.1.2 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) *In Labeled Security Mode: The sensitivity label associated with a subject shall be within the clearance range of the user;*
- b) *A started task executes with the user ID defined in the started class or started procedures table defining the started task.*

- c) **The DB2 primary authorization ID is initialized when the user makes a connection request. A DB2 agent is created for a user request that executes with the ID of the requesting user.**

FIA_USB.1.3 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 connection is established, the associated trusted context can:**
- **change the DB2 primary authorization ID,**
 - **assign a new sensitivity label associated with the subject,**
 - **assign a database role.**

Application note 1: 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 z/OS user ID.

Application note 2: A trusted context can assign a sensitivity label, a database role or a new user ID for each specific user defined in the trusted context or as a general assignment rule for the trusted connection.

6.1.4 Security management (FMT)

6.1.4.1 Management of security functions behavior (FMT_MOF.1)

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 Management of security attributes in DB2 (FMT_MSA.1(DB2-1))

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 Management of object security attributes for DB2 rows (FMT_MSA.1(DB2-2)) (Labeled Security Mode only)

FMT_MSA.1.1 The TSF shall enforce the ***Mandatory Access Control policy*** to restrict the ability to ***modify the sensitivity label associated with an object (a row in a table)*** to **users with the write-down privilege**.

Application note: This requirement applies to modification of a security label of a row in a table only. Changing the security label of a RACF profile for a DB2 object requires the user to have the SPECIAL attribute.

6.1.4.4 Static attribute initialization in DB2 (FMT_MSA_(EXT).3)

FMT_MSA_(EXT).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 ***Discretionary Access Control policy***.

Application note 1: this SFR is partially covered by FMT_MSA.3(1) defined in [ZOSST]; it is presented here for a complete instantiation of the set of SFRs defined in [BR-DBMSPP].

Application note 2: The extended component defined in [BR-DBMSPP] does not include the list of dependencies, management or audit activities. As changes compared with FMT_MSA.3 are minimal, the ST author assumes that the definition in CC part 2 is still applicable.

6.1.4.5 Static attribute initialization for rows in DB2 tables and MAC (FMT_MSA.3(DB2-2)) (Labeled Security Mode only)

FMT_MSA.3.1 The TSF shall enforce the ***Mandatory Access Control policy*** to provide ***restrictive*** default values for security attributes that are used to enforce the ***Mandatory Access Control policy***.

FMT_MSA.3.2 The TSF shall allow the ***users with the write-down privilege*** to specify alternative initial values to override the default values when an object or information is created.

6.1.4.6 Management of TSF data (FMT_MTD.1(DB2))

FMT_MTD.1.1 The TSF shall restrict the ability to ***include or exclude*** the ***auditable events*** to ***authorized administrators***.

Application note: This functional requirement covers FMT_MTD.1 defined in [BR-DBMSPP].

6.1.4.7 Revocation (FMT_REV.1(1))

FMT_REV.1.1(1) The TSF shall restrict the ability to revoke ***security 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 immediate revocation of security-relevant authorizations; and***
- b) ***none.***

Application note: "Security attributes associated with the users" refers to the combined list of attributes defined in FIA_ATD.1(DB2) and FIA_ATD.1(z/OS). Revocation is handled by z/OS even for the attributes defined by DB2.

6.1.4.8 Revocation (FMT_REV.1(2))

FMT_REV.1.1(2) The TSF shall restrict the ability to revoke ***security attributes*** associated with the ***objects*** under the control of the TSF to ***the authorized administrator and database***

users as allowed by the Discretionary Access Control policy or (in Labeled Security Mode) the Mandatory Access Control policy.

FMT_REV.1.2(2) The TSF shall enforce the rules

- a) **The access rights associated with an object shall be enforced when an access check is made;**
- b) **Labeled Security Mode only: the rules of the Mandatory Access Control policy are enforced on all future operations.**

6.1.4.9 Specification of Management Functions (FMT_SMF.1(DB2))

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

- a) **creation and deletion of database roles;**
- b) **creation, modification and deletion of trusted contexts**

Application note: this SFR iteration covers FMT_SMF.1 defined in [BR-DBMSPP].

6.1.4.10 Security management roles in DB2 (FMT_SMR.1(DB2))

FMT_SMR.1.1 The TSF shall maintain the **user** roles:

- a) **authorized administrator;**
- b) **users authorized by the Discretionary Access Control policy to modify object security attributes;**
- c) **users authorized to modify their own authentication data; and**
- d) **in Labeled Security Mode: users authorized by the Mandatory Access Control policy to modify object security attribute;**
- e) **DB2 installation system administrator (Install SYSADM)**
- f) **DB2 system administrator (SYSADM)**
- g) **DB2 System Controller (SYSCTRL)**
- h) **DB2 installation system operator (Install SYSOPR)**
- i) **DB2 System Operator (SYSOPR)**
- j) **DB2 database administrator (DBADM)**
- k) **DB2 database controller (DBCTRL)**
- l) **DB2 database maintainer (DBMAINT)**
- m) **DB2 package administrator (PACKADM)**

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 connections.

6.1.5 Protection of the TOE security functions (FPT)

6.1.5.1 Inter-TSF basic TSF data consistency in DB2 (FPT_TDC.1(DB2)) (Labeled Security Mode only)

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret labels of rows in tables of DB2 databases when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use the columns defined with AS SECURITY LABEL in tables of DB2 databases when interpreting the TSF data from another trusted IT product.

6.1.5.2 Internal TSF consistency (FPT_TRC_(EXT).1)

FPT_TRC_(EXT).1.1 The TSF shall ensure that TSF data is consistent between parts of the TOE by providing a mechanism to bring inconsistent TSF data into a consistent state in a timely manner.

Application Note 1: This SFR is trivially met as the TOE does not contain physically separated components.

Application Note 2: The extended component defined in [BR-DBMSPP] does not include the list of dependencies, management or audit activities. As changes compared with FPT_TRC.1 are minimal, the ST author assumes that the definition in CC part 2 is still applicable.

6.1.6 TOE Access (FTA)

6.1.6.1 Basic limitation on multiple concurrent sessions (FTA_MCS.1)

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 an admin configurable number of sessions per user.

6.1.6.2 TOE access history (FTA_TAH_(EXT).1)

FTA_TAH_(EXT).1.1 Upon successful session establishment, the TSF shall store and retrieve the **date and time** of the last successful session establishment to the user.

FTA_TAH_(EXT).1.2 Upon successful session establishment, the TSF shall store and retrieve the ***date and time*** of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

Application Note: The extended component defined in [BR-DBMSPP] does not include the list of dependencies, management or audit activities. As changes compared with FTA_TAH.1 are minimal, the ST author assumes that the definition in CC part 2 is still applicable.

Application Note: Successful and unsuccessful session establishment is recorded with the system's auditing. The date of the last successful session establishment is shown to the user during interactive, TSO/E based logons only.

6.1.6.3 TOE session establishment (FTA_TSE.1)

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/or group identity, time of day, day of the week, and none.***

Application note: This SFR is covered by z/OS: RACF can restrict session establishment based on time of day, day of week by user. It does not have this ability by group. This SFR is also only applicable to interactive, TSO/E based logons.

6.2 Security Requirements for the IT Environment

6.2.1 IT Environment (FIT)

6.2.1.1 IT Environment Protection Profile Compliance (FIT_PPC_(EXT).1)

FIT_PPC_(EXT).1.1 The IT environment shall be compliant with the requirements of the Controlled Access Protection Profile or an Operating System Protection Profile at the Basic Level of Robustness or Greater.

Application Note 1: The TOE consists of DB2 v9.1 for z/OS running on the z/OS V1R10 operating system, which was evaluated under the Common Criteria and compliant with the Controlled Access Protection Profile. Therefore, the definition of the TOE itself meets this requirement.

Application Note 2: The extended component defined in [BR-DBMSPP] does not include the list of dependencies, management or audit activities. As this requirement is axiomatic and is stated with the sole purpose of requiring an underlying platform, the ST author concludes that dependencies do not exist, and audit and management activities are not needed.

6.3 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.

6.3.1 Internal consistency and mutual support of SFRs

This section describes the mutual support and internal consistency of the components selected for this Security Target. These properties are discussed for both functional and assurance components.

Assignment, selection, and refinement operations were carried out among components using consistent computer security terminology. This helps to avoid the ambiguity associated with interpretations of meanings of terms between related components.

Multiple instantiation of identical or hierarchically-related components was used to clearly state the required functionality that must exist in a TOE conformant with this profile.

For internal consistency of the requirements, the following rationale is provided:

Auditing

The requirements for auditing have been completely derived from [BR-DBMSPP] and [CAPP]. The rationale for those requirements is:

FAU_GEN.1 defines the events that the z/OS part of the TOE is required to be able to audit. Those events are related to the other security functional requirements showing which event contributes to make users accountable for their actions with respect to the requirement. This covers also all those events related to DB2 that RACF audits. Those events include identification and authentication of users accessing DB2 via the DRDA interface, DB2 access checks performed by RACF and management of DB2 access rights (which is performed using the RACF commands).

FAU_GEN.1(DB2) defines some additional events captured by the DB2 trace mechanism. Since the DB2 trace mechanism also uses SMF to store the audit records it generates, the protection and management of the audit trail does not differ between the events generated by z/OS/RACF and the events generated by DB2. Note that this iteration also covers FAU_GEN.1-NIAP-0410 defined in [BR-DBMSPP].

FAU_GEN.2 requires that the events are associated with the identity of the user that caused the event. The identity has been associated with the subject that causes an auditable event by FIA_USB.1. Of course this can only be accomplished if the user is already known, which may not be the case for failed login attempts. Note that this iteration also covers FAU_GEN.2-(EXT).2 defined in [BR-DBMSPP] that takes into account this limitation.

FAU_SAR.1 ensures that authorized administrators are able to evaluate the audit records, while FAU_SAR.2 requires that no other users can read the audit records (because they may contain sensitive information). Taking into account that the amount of audit records gathered may be very large, FAU_SAR.3 requires that the TOE provides the ability to search the audit records for a set that satisfies defined attributes.

To avoid all possible audit records always being generated (which would result in an unacceptable overhead to the system performance and might easily fill up the available audit trail space) the TOE is required in FAU_SEL.1 (for z/OS) and FAU_SEL.1(DB2) to provide the possibility to restrict the events to be audited based on a set of defined attributes. Events audited by RACF as the result of attempted or performed access to DB2 objects are also configurable using the defined criteria. Note that this iteration also covers FAU_SEL.1-NIAP-0407 defined in [BR-DBMSPP], which requires that this functionality be available only to administrators.

Requirement FAU_STG.1 defines that audit records need to be protected from unauthorized deletion and modification to ensure their completeness and correctness. Requirement FAU_STG.3 addresses the aspect that the system detects a shortage in the audit trail space. This can be used to take preventive action, e.g. backup the audit trail and release the space to avoid a critical situation.

FAU_STG.4 addresses the problem that the TOE might not be able to record further audit records (e. g. due to the shortage of some resources). Also in this case the TOE needs to ensure that such a situation cannot be misused by a user to bypass the auditing of critical activities. Otherwise a user might deliberately bring the TOE into a situation where it is no longer able to audit critical events just to avoid that a critical action he performs is audited.

Because accountability also requires the ability to prove when and in which sequence security relevant events occurred, FPT_STM.1 provides for a reliable time reference.

Management of audit is addressed by FMT_MTD.1(1) for the audit trail, and FMT_MTD.1(2) and FMT_MTD.1(DB2) for the audited events.

Discretionary access control

FDP_ACC.1 requires the existence of a Discretionary Access Control Policy for named objects in z/OS, including named objects within the UNIX realm. The rules of this policy are described in FDP_ACF.1(1), FDP_ACF.1(2) and FDP_ACF.1(3) in iterations for UNIX, LDAP and non-UNIX and non-LDAP objects. FDP_ACC.1(DB2) defines the discretionary access control policy for DB2 objects and FDP_ACF.1(DB2) defines the rules for access to those objects. Discretionary access control rules are partly based on user security attributes provided through FIA_ATD.1(DB2). Management of (discretionary) access rights is defined in FMT_MSA.1(1), FMT_MSA.1(DB2-1) and FMT_REV.1. When initialized, object attributes are initialized to restrictive values (FMT_MSA.3(1) and FMT_MSA_(EXT).3), to avoid breaches of the security policy.

Because access decisions are based on user attributes, subjects must be bound to users on whose behalf they take action (FIA_USB.1 and FIA_USB.1(DB2)). This must be supported by proper identification and authentication.

Discretionary access control is also supported by the requirements for residual information protection, which prevent users from accessing information they are not authorized to by way of residual information remaining in objects that they allocate.

Mandatory access control (Labeled Security Mode only)

FDP_IFC.1 and FDP_IFC.1(DB2) require the existence of a mandatory access control policy for named objects in z/OS and DB2. Within DB2 mandatory access control is at the granularity of rows in tables of DB2 databases. The rules of this policy are described in FDP_IFF.2 and they apply for all objects that are subject to mandatory access control. Mandatory access control rules are partly based on user security attributes provided through FIA_ATD.1 and FIA_ATD.1(DB2). Management of labels attached to objects is defined in FMT_MSA.2 and FMT_REV.1(2). When new objects are created, proper attribute initialization is ensured by FMT_MSA.3(2) for z/OS objects and FMT_MSA.3(DB2-2) for DB2 objects.

Import and export of labeled and unlabeled data (FDP_ETC.1, FDP_ETC.2, FDP_ITC.1 and FDP_ITC.2) can be provided over a trusted channel (FTP_ITC.1). FPT_TDC.1 ensures that labels can be consistently interpreted when labeled data is transferred from one system to another (provided the two systems have been configured with compatible definitions of the security labels).

Because access decisions are based on user attributes, subjects must be bound to users on whose behalf they take action (FIA_USB.1 and FIA_USB.1(DB2)). This must be supported by proper identification and authentication.

Mandatory access control is also supported by the requirements for residual information protection, which prevent users from accessing information they are not authorized to by way of residual information remaining in objects that they allocate.

Identification and authentication

Identification and authentication are required for discretionary and mandatory access control as well as for auditing, which are based on the identity of individual users. FIA_UAU.1, FIA_UAU1(DB2), FIA_UID.1 and FIA_UID.1(DB2) require that users are authenticated before they can perform any critical action on the TOE. FIA_SOS.1 ensures that the mechanism used for authentication (passwords) has a minimum strength. FIA_UAU.7 provides some level of protection against simple spoofing in the TOE environment. FIA_USB.1 and FIA_USB.1(DB2) ensure that a TOE subject (z/OS task or DB2 agent) is properly bound to the user for whom it runs. This association also provides the user attributes (defined by FIA_ATD.1 and

FIA_ATD.1(DB2)) necessary to take policy decisions. Management of the user attributes and authentication data is provided by FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(DB2) and FMT_REV.1(1).

Additionally, FTA_TAH_(EXT).1 requires that users be informed about the last successful and unsuccessful session establishment; FTA_TSE.1 prevents users to establish sessions depending on date and time, and FTA_MSC.1 limits the number of concurrent sessions for a given user.

Object reuse

Object reuse (as required by FDP_RIP.2 and Note 1) is a supporting function that prevents unauthorized access to information through residuals left in objects when they are reallocated to another subject or object.

Object reuse therefore supports the intention of the discretionary and (in Labeled Security Mode) mandatory access control policies as well as identification and authentication and secure communication (for the protection of keys and data).

Security management

The functions defined so far require several management functions as defined by FMT_SMF.1.

Management of access rights and (in Labeled Security Mode) labels attached to objects is necessary to configure the DAC and (in Labeled Security Mode) MAC mechanisms; it is defined by FMT_MSA.1 and FMT_REV.1(2) "Revocation of Object Attributes". In addition new objects are required to have default access rights and security labels which are required by FMT_MSA.3.

Management of users and groups is defined in FMT_MTD.1(3) "Management of User Attributes" and FMT_REV.1(1) "Revocation of User Attributes". Because passwords are used for authentication, the management of authentication data is also required in FMT_MTD.1(4) "Management of Authentication Data".

Management of the audit system is covered by the requirements for the management of the audit trail (FMT_MTD.1(1)) and the management of the audit events (FMT_MTD.1(2) and FMT_MTD.1(DB2)). Audit trail management is supported by the requirements for the audit review (FAU_SAR.1 and FAU_SAR.3) as well as the requirements for the protection of the audit trail (FAU_STG.3 and FAU_STG.4). Management of the audit events is supported by the ability to select the events to be audited (FAU_SEL.1 and FAU_SEL.(DB2)).

In addition the TOE supports several roles, which is expressed by FMT_SMR.1.

Security management requirements therefore provide support for auditing, discretionary and (in Labeled Security Mode) mandatory access control, and identification and authentication.

TSF protection

The TOE needs to ensure that users are limited in their activities by the boundaries defined by the access control policies. To ensure this the TSF need to check all access of subjects to protected objects and maintain a domain for its own execution that protects it from interference and tampering by any subject that is not part of the TSF. This is expressed by the security requirement for the operational environment FIT_PPC_(EXT).1

As required by the before mentioned security requirement, DB2 relies on z/OS for this protection. The underlying hardware of the TOE performs extensive and continuous self tests to ensure the correct operation of the TOE. In the case when an error is detected, the TOE is informed by way of a machine-check interrupt about the problem, allowing the TOE to react to the error like shut down in a controlled way (provided the error does not lead to an immediate stop of the machine).

Secure communication

The TOE provides a protocol that allows applications or users to securely communicate with other trusted IT products (which may be other instantiations of the TOE). This protocol uses cryptographic functions to ensure the confidentiality and integrity of the user data during transmission as required. The requirements for those cryptographic functions are defined in FCS_CKM.1, FCS_CKM.2 and FCS_COP.1.

The protocol provides the ability to establish an Inter-TSF trusted channel, as required by FTP_ITC.1. Within this channel, user data transferred is protected for confidentiality (as required by FDP_UCT.1) and integrity (as required by FDP_UIT.1).

The secure generation of cryptographic keys used for secure communications is addressed by FMT_MSA.2.

6.3.2 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement defined in this ST addresses at least one security objective:

SFR	[ZOSST] and [CAPP] security objectives	[BR-DBMSPP] security objectives
FAU_GEN.1(DB2)	O.AUDITING	O.AUDIT_GENERATION
FAU_GEN_(EXT).2	O.AUDITING	O.AUDIT_GENERATION
FAU_SEL.1(DB2)	O.AUDITING O.MANAGE	O.AUDIT_GENERATION
FDP_ACC.1(DB2)	O.DISCRETIONARY_ACCESS	O.MEDIATE
FDP_ACF.1(DB2)	O.DISCRETIONARY_ACCESS	O.MEDIATE
FDP_ETC.1	O.MANDATORY_ACCESS	
FDP_ETC.2	O.MANDATORY_ACCESS	
FDP_IFC.1(DB2)	O.MANDATORY_ACCESS	
FDP_IFF.2	O.MANDATORY_ACCESS	
FDP_ITC.1	O.MANDATORY_ACCESS	
FDP_ITC.2	O.MANDATORY_ACCESS	
FDP_RIP.2	O.RESIDUAL_INFORMATION	O.RESIDUAL_INFORMATION
FDP_UCT.1	O.COMPROT	
FDP_UIT.1	O.COMPROT	
FIA_ATD.1(DB2)	O.AUTHORIZATION, O.DISCRETIONARY_ACCESS, O.MANDATORY_ACCESS	O.TOE_ACCESS
FIA_UAU.1(DB2)	O.AUTHORIZATION	
FIA_UID.1(DB2)	O.AUTHORIZATION	
FIA_USB.1(DB2)	O.AUTHORIZATION, O.DISCRETIONARY_ACCESS, O.MANDATORY_ACCESS, O.AUDITING	
FMT_MOF.1		O.MANAGE

FMT_MSA.1(DB2-1)	O.DISCRETIONARY_ACCESS, O.MANAGE	O.MANAGE
FMT_MSA.1(DB2-2)	O.MANDATORY_ACCESS, O.MANAGE	
FMT_MSA_(EXT).3	O.DISCRETIONARY_ACCESS, O.MANAGE	O.MANAGE
FMT_MSA.3(DB2-2)	O.MANDATORY_ACCESS, O.MANAGE	
FMT_MTD.1(DB2)	O.AUDITING, O.MANAGE	O.MANAGE
FMT_REV.1(1)	O.AUTHORIZATION, O.MANAGE	O.MANAGE
FMT_REV.1(2)	O.DISCRETIONARY_ACCESS, O.MANDATORY_ACCESS, O.MANAGE	O.MANAGE
FMT_SMF.1(DB2)	O.MANAGE	O.MANAGE
FMT_SMR.1(DB2)	O.MANAGE	O.MANAGE, O.ADMIN_ROLE
FPT_TDC.1(DB2)	O.MANDATORY_ACCESS	
FPT_TRC_(EXT).1		O.MEDIATE
FTA_MCS.1		O.TOE_ACCESS
FTA_TAH_(EXT).1		O.TOE_ACCESS, O.ACCESS_HISTORY
FTA_TSE.1		O.TOE_ACCESS

Table 12 - Mapping between SFRs and Security Objectives

6.3.3 Sufficiency

The security objectives defined in this ST have been defined in [ZOSST], [CAPP] and [BR-DBMSPP]. Please refer to these documents for the rationale that demonstrates the security functional requirements are suitable and sufficient to meet the security objectives.

6.3.4 Security requirements dependency analysis

The following table shows the dependencies of SFRs modeled in [CAPP] and CC Part 2 for the SFRs defined in this ST, and how the TOE resolves these dependencies.

Note that [BR-DBMSPP] has not modeled the SFR dependencies for extended components FAU_GEN_(EXT).2, FMT_MSA_(EXT).3, FPT_TRC_(EXT).1 and FIT_PPC(EXT).1; this is a known inconsistency in the protection profile. However, Table 15 “Functional Requirement Dependencies” in section 6.5 of [BR-DBMSPP] provides a meaningful and consistent set of dependencies for these extended components. This ST uses those dependencies.

Notice also that the dependencies for SFRs defined in [ZOSST] and not mentioned in this ST are not included.

Security Functional	Dependencies	Resolution
---------------------	--------------	------------

Requirement		DB2	z/OS
FAU_GEN.1(DB2)	FPT_STM.1		FPT_STM.1
FAU_GEN_(EXT).2	FAU_GEN.1 FAU_GEN.1-NIAP-0410	FAU_GEN.1(DB2)	FAU_GEN.1
	FIA_UID.1		FIA_UID.1
FAU_SEL.1(DB2)	FAU_GEN.1 FAU_GEN.1-NIAP-0410	FAU_GEN.1(DB2)	FAU_GEN.1
	FMT_MTD.1	FMT_MTD.1(DB2)	
FDP_ACC.1(DB2)	FDP_ACF.1 FDP_ACF.1-NIAP-0407	FDP_ACF.1(DB2)	
FDP_ACF.1(DB2)	FDP_ACC.1 FDP_ACC.1-NIAP-0407	FDP_ACC.1(DB2)	
	FMT_MSA.3	FMT_MSA_(EXT).3, FMT_MSA.3(DB2-2)	FMT_MSA.3(1), FMT_MSA.3(2)
FDP_ETC.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1(DB2), FDP_IFC.1(DB2)	
FDP_ETC.2	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1(DB2), FDP_IFC.1(DB2)	
FDP_IFC.1(DB2)	FDP_IFF.1		FDP_IFF.2
FDP_IFF.2	FDP_IFC.1	FDP_IFC.1(DB2)	FDP_IFC.1
	FMT_MSA.3	FMT_MSA_(EXT).3, FMT_MSA.3(DB2-2)	FMT_MSA.3(1), FMT_MSA.3(2)
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1(DB2), FDP_IFC.1(DB2)	
	FMT_MSA.3	FMT_MSA_(EXT).3, FMT_MSA.3(DB2-2)	FMT_MSA.3(1), FMT_MSA.3(2)
FDP_ITC.2	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1(DB2), FDP_IFC.1(DB2)	
FDP_RIP.2	None		
FDP_UCT.1	[FDP_ACC.1 or FDP_IFC.1 or FDP_ITC.1]	FDP_ACC.1(DB2), FDP_IFC.1(DB2)	FDP_ITC.1
FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1 or FDP_ITC.1]	FDP_ACC.1(DB2), FDP_IFC.1(DB2)	FDP_ITC.1
FIA_ATD.1(DB2)	None		
FIA_UAU.1(DB2)	FIA_UID.1	FIA_UID.1(DB2)	

FIA_UID.1(DB2)	None		
FIA_USB.1(DB2)	FIA_ATD.1	FIA_ATD.1(DB2)	
FMT_MOF.1	FMT_SMF.1	FMT_SMF.1(DB2)	
	FMT_SMR.1	FMT_SMR.1(DB2)	
FMT_MSA.1(DB2-1)	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1(DB2)	
	FMT_SMF.1	FMT_SMF.1(DB2)	
	FMT_SMR.1	FMT_SMR.1(DB2)	
FMT_MSA.1(DB2-2)	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1(DB2)	
	FMT_SMF.1	FMT_SMF.1(DB2)	
	FMT_SMR.1	FMT_SMR.1(DB2)	
FMT_MSA_(EXT).3	FMT_MSA.1	FMT_MSA.1(DB2-1)	
	FMT_SMR.1	FMT_SMR.1(DB2)	
FMT_MSA.3(DB2-2)	FMT_MSA.1	FMT_MSA.1(DB2-2)	
	FMT_SMR.1	FMT_SMR.1(DB2)	
FMT_MTD.1(DB2)	FMT_SMF.1	FMT_SMF.1(DB2)	
	FMT_SMR.1	FMT_SMR.1(DB2)	
FMT_REV.1(1)	FMT_SMR.1	FMT_SMR.1(DB2)	
FMT_REV.1(2)	FMT_SMR.1	FMT_SMR.1(DB2)	
FMT_SMF.1(DB2)	None		
FMT_SMR.1(DB2)	FIA_UID.1	FIA_UID.1(DB2)	
FPT_TDC.1(DB2)	None		
FPT_TRC_(EXT).1	FPT_ITT.1	This dependency is not needed as FPT_TRC_(EXT).1 is trivially met by the fact that the TOE does not have separate parts.	
FTA_MCS.1	FIA_UID.1	FIA_UID.1(DB2)	
FTA_TAH_(EXT).1	None		
FTA_TSE.1	None		

Table 13- SFR Dependencies

6.3.5 Rationale for Demonstrable Conformance

As mentioned in previous sections, the TOE consists of DB2 for z/OS and the z/OS underlying platform, which has been already evaluated. The approach in this security target has been to reuse [ZOSST] and

add the necessary security functional requirements to conform both [CAPP] and [BR-DBMSPP] protection profiles. **Table 8** and **Table 10** show the security functional requirements included in this ST, and how operations have been performed in each of the protection profiles.

All security functional requirements defined in [CAPP] are completely covered in [ZOSST]. Additional iterations to these security functional requirements have been added as iterations to incorporate specific behavior for DB2.

All security functional requirements defined in [BR-DBMSPP] are completely covered in this Security Target.

There are security functional components that are defined in only one protection profile and not in the other. In all cases the security functional requirements do not collide with the set of components defined in the other protection profile.

There are several security functional components that are claimed in both protection profiles:

- components are similar and copied from CC part 2;
- components from CC part 2 but stated with different assignment and/or selection operations;
- components from CC part 2 with refinement operations;
- extended components

In all cases the approach has been to merge both components in a single security functional requirement maintaining the meaning from both protection profiles. The author has not found any inconsistency between the components from both protection profiles so the merging was possible in all cases.

Due to the fact that [CAPP] and [BR-DBMSPP] use security functional requirements from part 2 of CC version 2.3 that differ from the respective security functional requirements of CC version 3.1, a rewording of FAU_SEL.1, FMT_REV.1(1) and FMT_REV.1(2) was performed preserving their contents.

In CC 3.1 the wording of FAU_SAR.3 and FAU_STG.4. has been changed but this was not updated in [ZOSST]. Since with respect to FAU_SAR.3 performing searches is a method of selection and in FAU_STG.4 auditable events was replaced by audited events only, referencing to these SFRs is determined to be sufficient and the SFRs are not repeated and modified in this ST.

Finally, additional security functional components related to the Mandatory Access Policy for Labeled Security Mode are added in [ZOSST] and this ST from CC part 2, contributing to a more restrictive set of SFRs than the ones defined in the claimed protection profiles.

6.4 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. No operations are applied to the assurance components.

6.5 Security Assurance Requirements Rationale

The evaluation assurance level 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 stated in [CAPP] and [BR-DBMSPP].

6.6 TOE Summary Specifications Rationale

6.6.1 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. Notice that only the SFR defined in this Security Target are included in this mapping; for the mapping of the SFRs defined for the z/OS underlying platform please refer to section 5.4.1 in [ZOSST].

SFR	Security Functions
FAU_GEN.1(DB2)	Section 7.6.1 explains how DB2 makes use of the auditing features of z/OS and generates specific records for DB2. Further explanation of the auditing functionality can be found in section 6.6.1 of [ZOSST].
FAU_GEN_(EXT).2	Section 7.6.1 explains the information contained in the audit records and tools that can be used to export them in human-readable format. Further explanation of the auditing functionality can be found in section 6.6.1 of [ZOSST].
FAU_SEL.1(DB2)	Sections 6.6.3 and 6.5.1.8 in [ZOSST] explains how the auditor role can configure the events that are audited. These sections also explain that the owner of a profile can define which events related to the profile are audited.
FDP_ACC.1(DB2)	The general operation of access control for DB2 is explained in Section 7.3.4. The administrative authorities for DB2 are explained in section 7.3.4.3 and the privileges for the different DB2 objects are explained in sections 7.3.4.4 through 7.3.4.19.
FDP_ACF.1(DB2)	Section 7.3.4.2 explains the access control for DB2 objects.
FDP_ETC.1	Export of non-labeled user data, e.g. tables without security labels, is performed by tapes or through network connections. It is not mentioned explicitly that those connections can be used for this purpose, but this should be clear. Access control to these export channels is explained in section 6.3.2 of [ZOSST].
FDP_ETC.2	Export of labeled data is explained in Section 7.3.3.1. Further explanation can be found in section 6.3.3 of [ZOSST].
FDP_IFC.1(DB2)	The mandatory access control policy for DB2 is explained in Section 7.3.3.1. Further explanation can be found in section 6.3.3 of [ZOSST].
FDP_IFF.2	The mandatory access control policy for DB2 is explained in Section 7.3.3.1. Further explanation can be found in section 6.3.3 of [ZOSST].
FDP_ITC.1	Import of unlabeled user data is the inverse of export and is explained in the same section as the export (section 6.3.2 of [ZOSST]).
FDP_ITC.2	Import of labeled user data is the inverse of export and is explained Section 7.3.3.1. Further explanation can be found in section 6.3.3 of [ZOSST].
FDP_RIP.2	Object reuse for DB2 objects is described in section 7.7.2; object reuse for z/OS objects is described in Section 6.7 of [ZOSST].
FDP_UCT.1	Confidentiality in data communications is explained in section 6.4 of [ZOSST].
FDP_UIT.1	Integrity in data communications is explained in section 6.4 of [ZOSST].
FIA_ATD.1(DB2)	Section 7.2.2 describes the concept of trusted context associated with a user, section 7.3.4.3 explains the concept of administrative authorities (user roles) in DB2; other user attributes are also used in z/OS and are described in sections 6.5.1.1 through 6.5.1.4 and 6.5.1.8 of [ZOSST].
FIA_UAU.1(DB2)	User authentication to DB2 is explained in sections 7.2.1 and 7.2.2. Further explanation can be found in sections 6.2.1 through 6.2.5, 6.2.6 and 6.2.8 in

	[ZOSST].
FIA_UID.1(DB2)	User identification to DB2 is explained in sections 7.2.1 and 7.2.2. Further explanation can be found in section 6.2 in [ZOSST].
FIA_USB.1(DB2)	User subject binding for trusted connections in DB2 is explained in section 7.2.2. For the rest of the user attributes, refer to section 6.2 in [ZOSST].
FMT_MOF.1	Section 6.6.1 in [ZOSST] explains that the administrator can configure RACF and other elements of the TOE to control generation of the audit records.
FMT_MSA.1(DB2-1)	Management of object security attributes is explained in section 6.5.2 (and subsections) of [ZOSST] where the different RACF profiles and their management is described, along with descriptions for z/OS UNIX objects and LDAP LDBM objects. Section 6.5.3 in [ZOSST] explains the RACF configuration.
FMT_MSA.1(DB2-2)	DB2 security management is explained in section 7.5.2. Additionally, section 7.3.3.1 explains that the write-down privilege is required to change the label for a row in a DB2 table.
FMT_MSA_(EXT).3	Default values for the access control are defined in the UACC attribute in the resource profiles as explained in section 6.5.2 (and subsections) of [ZOSST] in the description of the resource profiles. Defaults for z/OS UNIX and LDAP LDBM objects are discussed in sections 6.5.2.3 and 6.5.2.4 of [ZOSST].
FMT_MSA.3(DB2-2)	DB2 security management is explained in section 7.5.2. The mandatory access control based on the labels of rows in DB2 tables is explained in section 7.3.3.1
FMT_MTD.1(DB2)	Audit event management is explained in section 6.6 of [ZOSST].
FMT_REV.1(1)	Revocation of user attributes is explained as part of the management of user attributes in section 6.5.1 in [ZOSST].
FMT_REV.1(2)	Revocation of object attributes is explained as part of the management of access control to objects in sections 6.3.2 (DAC) and 6.3.3 (MAC) of [ZOSST]. These sections do not explicitly mention how to revoke DB2 object attributes but since they are also managed by RACF it is obvious that the same RACF commands as for z/OS objects are also used for DB2 objects.
FMT_SMF.1(DB2)	Security management functions in DB2 are described in section 7.5.2.
FMT_SMR.1(DB2)	DB2 user roles (known as administrative authorities in DB2) are explained in sections 7.3.4.3 and 7.5.3. Other user roles are explained in section 6.5.1.8 of [ZOSST]
FPT_TDC.1(DB2)	The capability to provide inter-TSF data consistency for labels of rows in tables of DB2 databases is explained with the description of the mandatory access control in section 7.3.3.1.
FPT_TRC_(EXT).1	This SFR is trivially met as the TOE does not contain physically separated components.
FTA_MCS.1	Limitation on the number of concurrent sessions per user is explained in section 7.2.2
FTA_TAH_(EXT).1	Storage and retrieval of the user access history is explained in section 7.2.2
FTA_TSE.1	Session establishment is explained in section 7.2.1

Table 14 - 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 extends 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 platform; the new 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 architecture

DB2 is a database management system operating on top of z/OS and z/OS is an operating system that runs on the IBM z/Architecture processors. Those processors provide a separate problem and supervisor state and 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. z/OS provides the capability for applications to execute in separate and protected address spaces and DB2 uses this to establish a domain for its own execution that is protected from direct access by untrusted applications executing on top of z/OS. 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. In Labeled Security Mode: mandatory access control based on security attributes of subjects and objects
4. Management functions to administer auditing, discretionary access control, and (in Labeled Security Mode) mandatory access control, as well as users and groups with their related attributes
5. An audit trail for security relevant events
6. Secure communication
7. Object reuse
8. TOE self-protection functions based on security features provided by the underlying hardware including memory protection and the provision of a privileged state that allows the TOE to reserve and protect a domain for its own execution

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

z/OS also supports UNIX terminals through telnet, rlogin, and other TCP/IP-based network protocols.

DB2 is structured into the following major units:

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

The TOE itself consists of a “nucleus” 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. Therefore, all authorized programs allowed to be executed in the evaluated configuration are considered to be part of the TOE. DB2 operates as a set of “trusted processes” on top of z/OS.

More information on how the TOE identifies, manages, and protects authorized programs can be found in Section 7.6.

7.1.1 Main trusted subsystems of the evaluated configuration

Some programs are started with authorization (see also section 7.10) during system startup. Those include the Job Entry Subsystem (JES2), the Time Sharing Option Extensions (TSO/E) subsystem, the Communication Subsystem (CS), the z/OS UNIX System Services, and the DB2 subsystem.

The functionality of the JES2, the TSO/E subsystem, the Communications Server and the z/OS UNIX System Services is described in [ZOSST] section 6.1.1.

7.1.1.1 DB2

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.

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.

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
- As a user through a trusted connection, authorized by the association with a trusted context (see next section).
- Through an external entity that establishes a trusted connection, authorized by the association with a trusted context (see next section)

In all cases, users are identified and authenticated by a user ID and password combination (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).

Access to the TOE can also be restricted by user identity, time of day and day of week. This functionality is provided by RACF (IA.1.3).

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 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 authorization ID (IA.4-DB2-1).

Users connecting using the external DRDA interface will have to present a valid user ID and password. DB2 uses RACF to validate the user's password and will allow the user to perform any other action only after he has been successfully authenticated (IA.4-DB2-2).

When a session is established, the TOE provides access history information: the date and time of the last successful session and all unsuccessful attempts since the last successful session are shown to the user (IA.4-DB2-3).

DB2 can also limit the number of concurrent sessions per user through a configurable parameter (IA.4-DB2-4).

7.2.3 Trusted connections

Additionally, a user or user application can interact with the TOE through what is known as a "trusted connection". A trusted connection, 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 DB2 primary authorization ID used to establish the connection: the USER parameter included in the JOB statement (for BATCH or RRSF), the RACF user id (for RRSF) 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 can be trusted based on:

- The system authorization ID which is determined either by a set of rules included in the SYSIBM catalog tables² (for z/OS requesters), derived from the authentication token (for z/OS servers³), 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 or a security label (in Label Security Mode) depending on the rules defined in the trusted context (IA.4-DB2-7).

7.3 Access control

7.3.1 Access control principles

z/OS provides 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 and (in Labeled Security Mode) 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 non-UNIX resource like DB2 objects.

Access to DB2 objects is 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 and profiles in those classes are used to protect the DB2 resources.

In addition DB2 uses RACF for row-level security to check the right of the user to access a field in a row based on the labels for mandatory access control. RACF checks if the current security label of the user allows the type of access based on the security label of the row and the rules of mandatory access control. For discretionary control access, there is no RACF controlled access at row level but only at table and view levels.

Access control is also implemented in trusted connections, 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, a security label 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.
- In Labeled Security mode, the security label assigned to the trusted connection is used for enforcing mandatory access control.

² For more information, see “Establishing remote trusted connections by DB2 for z/OS requesters” in the DB2 Administration Guide.

³ For more information, see “Establishing remote trusted connections to DB2 for z/OS servers” in the DB2 Administration Guide.

- Assigning a different user to the trusted connection forces the discretionary access control using the access rights of the impersonated user.

7.3.2 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 security label, 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 Mandatory access control (Labeled Security Mode only)

7.3.3.1 Mandatory access control in DB2

DB2 allows for mandatory access control based on the labels of rows in tables. A table needs to be defined with one column for the security label. This is done using the AS SECURITY LABEL operand in the CREATE TABLESQL statement⁴. The security label is then defined and controlled by the TOE in accordance with the rules for mandatory access control (AC.3-DB2-1).

When a user accesses a row or a field in the row with some SQL statement, DB2 calls RACF to check if the user is allowed to perform the type of access based on the mandatory access control rules. The operation will only be successful if the user has the requested access right to all of the rows containing fields that are accessed as part of the SQL statement he performs. Especially when the user accesses data using a view he may access specific fields of row within a table. For all fields accessed DB2 needs to check the security label of the row containing the field and deny access when for one or more fields the user is not allowed to perform the type of access requested based on the mandatory access control rules (AC.3-DB2-2).

In a trusted connection, a security label can be assigned to the process, either as a global value or a specific value for the user id, depending on the trusted context definition. Mandatory access control rules are enforced using this security label.

The security label of a row is initialized with the security label of the process creating the row (using the INSERT SQL statement) (AC.3-DB2-3). User with the write-down privilege can specify a different label than their current one when they create a row (AC.3-DB2-4).

⁴ The ALTER TABLE SQL statement also supports the AS SECURITY LABEL clause, but its usage is not possible in a CC evaluation configuration as all tables must possess a security label when created and cannot be changed.

A user with the write-down privilege can change the security label of an existing row in a table with the UPDATE SQL statement (AC.3-DB2-5).

Since the security labels of rows of a DB2 table are stored in a dedicated column of the table, the security labels are also exported when the database is exported (AC.3-DB2-6). The system importing the labeled data must have security labels defined compatible with those of the exporting system to allow the consistent interpretation of the labels.

7.3.4 Discretionary access control in DB2

7.3.4.1 DB2 objects

Discretionary access control to RACF resources is controlled by the user, group, role, and resource profiles stored and managed by RACF. Role is only considered when a trusted connection is established.

Access control is defined for DB2 objects. The following list shows the DB2 objects and their hierarchy:

- Subsystem or data sharing group
 - Database
 - Table space
 - Table
 - Column
 - Row
 - Index space
 - Index
 - View
- 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
 - Distinct type – not in evaluated configuration
 - Sequence
- Trusted context

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 role. In trusted connections, role ownership in DB2 objects and the role assigned to the process based on the trusted context definition are taken into account in the Discretionary Access Control policy. In non-trusted connections, only authorization ID ownership is used.

Note that rows are not objects that are subject to discretionary access control on their own. Discretionary access control is at the granularity of a table or a column.

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, 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 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 Class to control access to DB2 subsystems
- GDSNBP or MDSNBP Class to control access to DB2 buffer pools
- GDSNCL or MDSNCL Class to control access to DB2 collections
- GDSNDB or MDSNDB Class to control access to DB2 databases
- GDSNJR or MDSNJR Class to control access to DB2 Java archive files
- GDSNPK or MDSNPK Class to control access to DB2 packages
- GDSNPN or MDSNPN Class to control access to DB2 plans
- GDSNSC or MDSNSC Class to control access to DB2 schemata
- GDSNSG or MDSNSG Class to control access to DB2 storage groups
- GDSNSM or MDSNSM Class to control DB2 privileges
- GDSNSP or MDSNSP Class to control access to DB2 stored procedures
- GDSNSQ or MDSNSQ Class to control access to DB2 sequences
- GDSNTB or MDSNTB Class to control access to DB2 tables, indexes or views
- GDSNTS or MDSNTS Class to control access to DB2 table spaces

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	<i>bufferpool-name</i>
Collection	<i>collection-ID</i>
Database	<i>database-name</i>
Java archive (JAR)	<i>schema-name.JAR-name</i>
Package	<i>collection-ID.package-ID</i> <i>collection-ID</i> <i>owner</i>
Plan	<i>plan-name</i> <i>owner</i>

DB2 object	Object name qualifiers
Role	not applicable
Schema	<i>schema-name</i> <i>schema-name.function-name</i> <i>schema-name.procedure-name</i> <i>schema-name.type-name</i>
Sequence	<i>schema-name.sequence-name</i>
storage group	<i>storage-groupname</i>
stored procedure	<i>schema-name.procedure-name</i>
System	<i>owner</i>
table, index	<i>table-qualifier.table-name</i> <i>table-qualifier.table-name.column-name</i>
table space	<i>database-name.table-space-name</i>
trusted context	not applicable
user-defined distinct type	<i>schema-name.type-name</i>
user-defined function	<i>schema-name.function-name</i>
View	<i>view-qualifier.view-name</i>

Table 15: 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.

7.3.4.2 Access evaluation algorithm for DB2 objects

In the evaluated configuration access to DB2 privileges and authorities is granted either because of the implicit privileges in a DB2 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 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 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 has to a DB2 privilege or authority to a DB2 object:

1. If the user has a specific DB2 authority, granted by the implicit rights of a DB2 role, access is granted (AC.4-DB2-1)
2. If the user is the owner of the DB2 object and the requested DB2 authority is granted to the owner of the object, access is granted (AC.4-DB2-2a)
3. In a trusted connection, if there is a database role assigned, the database role is the owner of the DB2 object and the requested DB2 authority is granted to the owner of the object, access is granted (AC.4-DB2-2b)
4. If the user (as defined by the primary authorization ID) has sufficient access authority (see Note) in the standard access list of the RACF profile protecting the requested authority to the DB2 object, access is granted (AC.4-DB2-3).
5. If the user (as defined by the primary authorization ID) has sufficient access authority (see Note) in the standard access list of the RACF profile protecting any type of DB2 privilege that allows access (according to the description in sections 6.3.6.4 to 6.3.6.16), access is granted (AC.4-DB2-4).
6. If the current group of the user has sufficient access authority (see Note) 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 (see Note) in the standard access list of the RACF profile protecting any type of DB2 privilege that allows access (according to the description in sections 7.3.6.4 to 7.3.6.16), 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 (see Note) 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 (see Note) in the standard access list of the RACF profile protecting any type of DB2 privilege that allows access (according to the description in sections 6.3.6.4 to 6.3.6.16), 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 (see Note) 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 6.3.6.4 to 6.3.6.16) provides sufficient access (see Note) 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 6.3.6.4 to 6.3.6.16) provides sufficient access (see Note) 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 (see Note), 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 (see Note), 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 (see Note), access is granted (AC.4-DB2-18).
18. If none of those conditions has granted access, access is denied (AC.4-DB2-19).

Note 1: Sufficient access differs depending on whether the RACF MLS option is active or inactive:

- If the RACF MLS option is not active, a user with at least READ authorization to the resource has sufficient access.
- If the RACF MLS option is active and the request is not a write request, a user with at least READ authorization to the resource has sufficient access.
- If the RACF MLS option is active, and the request involves a write request, a user at least UPDATE authorization to the resource has sufficient access.

Note 2: Trusted connections allow the assignment of a different primary authorization ID, a database role or a security label 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 (database role is only valid in trusted connections).

7.3.4.3 DB2 administrative authorities

Administrative authorities are defined similar 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 the related objects:

Administrative authority	RACF object qualifier
DBADM	<i>database-name</i>
DBCTRL	<i>database-name</i>
DBMAINT	<i>database-name</i>
PACKADM	<i>collection-ID</i>
SYSADM	—
SYSCTRL	—
SYSOPR	—

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 authority for the DB2 object that the user requires sufficient access to.

See the Note at the end of Section 'Access evaluation algorithm for DB2 objects' on page 69 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 7.5.3.

7.3.4.4 Buffer pool privileges

A user has USE authority to a buffer pool if:

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

or

- The user has sufficient access to *DB2-subsystem.SYSCTRL* in the DSNADM class (AC.4-DB2-21)

or

- The user has sufficient access to *DB2-subsystem.SYSADM* in the DSNADM class (AC.4-DB2-22)

7.3.4.5 Collection privileges

A user has CREATE IN authority to a collection if:

- The user has sufficient access to the resource *DB2-subsystem.collection-ID*.CREATEIN in the MDSNCL or GDSNCL class (AC.4-DB2-23)

or

- The user has sufficient access to the resource *DB2-subsystem.collection-ID*.PACKADM in the DSNADM class (AC.4-DB2-24)

or

- The user has sufficient access to *DB2-subsystem.SYSCTRL* in the DSNADM class (AC.4-DB2-25)

or

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

7.3.4.6 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

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	DBMAINT	DBCTRL	DBADM	SYSCTRL	SYSADM
CREATETAB	X	X	X	X	X	X
CHANGE NAME QUALIFIER:			X	X	X	X
CREATETS	X	X	X	X	X	X
DISPLAYDB ⁵	X	X	X	X	X	X

⁵ Also SYSOPR or DISPLAY in the DB2-subsystem class allow access

Privilege	Privilege in DB class	DBMAINT	DBCTRL	DBADM	SYSCTRL	SYSADM
DROP	X		X	X	X	X
IMAGCOPY, MERGECOPY, MODIFY RECOVERY, QUIESCE	X	X	X	X	X	X
RECOVERDB, REPORT	X		X	X	X	X
REORG	X		X	X	X	X
REPAIR, RUN REPAIR UTILITY	X		X	X	X	X
REPAIR DBD					X	X
RUN CHECK UTILITY, STATS	X	X	X	X	X	X
STARTDB	X	X	X	X	X	X
STOPDB	X	X	X	X	X	X
TERM UTILITY ⁶					X	X
TERM UTILITY ON DATABASE		X	X	X		

7.3.4.7 Java archive privileges

Java archives are not part of the evaluated configuration.

7.3.4.8 Package privileges

The following privileges are defined for DB2 packages:

- BIND
- COPY
- DROP
- EXECUTE

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 ⁷	Privilege in Package class	PACKADM	SYSCTRL	SYSADM
BIND	X	X	X	X	X
COPY	X	X	X	X	X
DROP			X	X	X
EXECUTE		X	X	X	X

⁶ Also SYSOPR in the DB2-subsystem class allows access

⁷ Object ownership includes both authorization ID and role ownership. Role ownership is only applicable when the process established a trusted connection.

7.3.4.9 Plan privileges

The following privileges are defined for DB2 plans:

- BIND
- EXECUTE

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	SYSCTRL	SYSADM
BIND	X	X	X	X
EXECUTE		X		X

7.3.4.10 Role privileges

The following privileges are defined for DB2 roles:

- COMMENT ON ROLE
- CREATE ROLE
- DROP DROLE

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
COMMENT ON	X		X	X
CREATE ROLE			X	X
DROP ROLE	X		X	X

7.3.4.11 Schema privileges

The following privileges are defined for DB2 schemata:

- ALTERIN
- CHANGE NAME QUALIFIER
- COMMENT ON
- CREATEIN
- DROPIN

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
ALTERIN	X	X	X	X	X
CHANGE NAME QUALIFIER				X	X

Schema Privilege	User name matches schema name	Schema Owner	Privilege in Schema class	SYSCTRL	SYSADM
COMMENT ON	X	X	X ⁸	X	X
CREATEIN	X		X	X	X
DROPIN	X	X	X	X	X

7.3.4.12 Sequence privileges

The following privileges are defined for DB2 sequences:

- ALTER
- COMMENT ON
- USAGE

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	SYSCTRL	SYSADM
ALTER	X	X	X ⁹	X	X
COMMENT ON	X	X	X ¹⁰	X	X
USAGE		X	X		X

7.3.4.13 Storage group privileges

The only storage group privileges are USE, DROP and ALTER. USE requires either sufficient access to the DB2-subsystem.storage-groupname.USE profile in the MDSNSG or GDSNSG class or SYSCTRL or SYSADM in the DSNADM class. DROP and ALTER both require that a user has SYSCTRL or SYSADM in the DSNADM class (AC.4-DB2-32).

7.3.4.14 Stored procedure privileges

The following privileges are defined for DB2 stored procedures:

- DISPLAY
- EXECUTE
- START
- STOP

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

⁸ The privilege name is ALTERIN

⁹ Or access to resource *schema-name*.ALTERIN

¹⁰ Or access to resource *schema-name*.ALTERIN

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

7.3.4.15 DB2 system privileges

The following privileges are defined for DB2 system in general:

- ALTER BUFFERPOOL
- BINDADD
- BINDAGENT
- CANCEL DDF, START DDF, STOP DDF, DISPLAY RLIMIT, START RLIMIT, STOP RLIMIT
- CREATEALIAS
- CREATEDBA
- CREATESG
- CREATETMTAB
- DEBUGSESSION
- DISPLAY, DISPLAY BUFFERPOOL
- DISPLAY ARCHIVE
- DISPLAY PROFILE
- MONITOR1
- MONITOR2
- RECOVER BSDS
- RECOVER INDOUBT
- SET ARCHIVE
- START PROFILE
- STOP PROFILE
- STOPALL
- STOSPACE UTILITY
- TRACE
- USE ARCHIVE LOG

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
ALTER BUFFERPOOL		X	X	X
BINDADD	X		X	X
BINDAGENT	X		X	X
CANCEL START STOP DDF DISPLAY START STOP RLIMIT		X	X	X
CREATEALIAS ¹¹	X		X	X
CREATEDBA	X ¹²		X	X
CREATESG	X		X	X
CREATETMTAB	X ¹³		X	X
DEBUGSESSION	X			X
DISPLAY, DISPLAY BUFFERPOOL	X ¹⁴	X	X	X
DISPLAY ARCHIVE	X ¹⁵	X	X	X
DISPLAY PROFILE		X	X	X
MONITOR1	X ¹⁶		X	X
MONITOR2	X		X	X
RECOVER BSDS	X		X	X
RECOVER INDOUBT	X	X	X	X
SET ARCHIVE	X	X	X	X
START PROFILE		X	X	X
STOP PROFILE		X	X	X
STOPALL	X	X	X	X
STOSPACE UTILITY	X		X	X
TRACE	X	X	X	X
USE ARCHIVE LOG	X ¹⁷		X	X

7.3.4.16 Table privileges

The following privileges are defined for tables:

¹¹ also DBCTRL or DBADM for the database in the DSNADM class provides permission.

¹² Two specific resource names CREATEDBA and CREATEDBC exist.

¹³ Two specific resource names CREATETMTAB and CREATETAB exist.

¹⁴ Authority to DISPLAY allows access.

¹⁵ Both authority to DISPLAY and the ARCHIVE allow access.

¹⁶ Both authority to MONITOR1 and MONITOR2 allow access.

¹⁷ The privilege name is ARCHIVE.

- ALTER
- ALTER INDEX, RENAME INDEX, DROP INDEX
- CHANGE NAME QUALIFIER
- COMMENT ON, COMMENT ON INDEX, DROP
- CREATE SYNONYM
- CREATE VIEW
- DELETE
- DROP ALIAS
- DROP SYNONYM
- INDEX
- INSERT
- LOAD
- LOCK TABLE
- REFERENCES
- RENAME TABLE
- SELECT
- TRIGGER
- REFRESH
- UPDATE

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 in database class	SYSCTRL	SYSADM
ALTER	X	X	X	X	X
ALTER INDEX, RENAME INDEX, DROP INDEX	X ¹⁸		X	X	X
CHANGE NAME QUALIFIER			X ¹⁹	X	X
COMMENT ON, COMMENT ON INDEX, DROP	X		X	X	X
CREATE SYNONYM ²⁰	X	X	X	X	X
CREATE VIEW ²¹	X ²²		X ²³	X ²⁴	X

¹⁸ Owner of the index.

¹⁹ Also DBCTRL in the database class allows access.

²⁰ There are no authorization checks for CREATE SYNONYM

²¹ SELECT on table or view is also sufficient.

²² Not allowed in Labeled Security mode because implicit ownership does not apply.

²³ Tables only, not views.

Table privilege	Owner of table	Privilege in Table class	DBADM in database class	SYSCTRL	SYSADM
DELETE	X	X	X	X ²⁵	X
DROP ALIAS	X			X	X
DROP SYNONYM ²⁶	X	X	X	X	X
INDEX	X	X	X	X	X
INSERT	X	X	X	X ²⁷	X
LOAD	X	X	X	X	X
LOCK TABLE ²⁸	X	X	X	X	X
REFERENCES	X	X ²⁹	X	X	X
REFRESH	X		X ³⁰	X ³¹	X
RENAME TABLE	X		X ³²	X	X
SELECT	X	X	X	X ³³	X
TRIGGER	X	X ³⁴	X	X	X
UPDATE	X	X	X	X ³⁵	X

7.3.4.17 Tablespace privileges

The following privileges are defined for table spaces:

- DROP, ALTER
- USE

For DROP and ALTER the user requires either sufficient access to the *DB2-subsystem.database-name*.DBADM profile in the DSNADM class or SYSCTRL or SYSADM for the DB2 subsystem in the DSNADM class (AC.4-DB2-36).

For USE the user requires either one of the privileges that allow DROP or ALTER or authority to the *DB2-subsystem.database-name.tablespace-name*.USE profile in the MDSNTS or GDSNTS class (AC.4-DB2-37).

²⁴ Only for system catalog tables

²⁵ Only for system catalog tables

²⁶ There are no authorization checks for DROP SYNONYM

²⁷ Only for system catalog tables

²⁸ SELECT on table is also sufficient.

²⁹ There are multiple privileges that allow access.

³⁰ DBCTRL also allows access.

³¹ This check is bypassed for user tables.

³² Also DBMAINT and DBCTRL allow access.

³³ Only for system catalog tables

³⁴ TRIGGER and ALTER allow access.

³⁵ Only for system catalog tables

7.3.4.18 Trusted context privileges

The following privileges are defined for DB2 trusted contexts:

- ALTER TRUSTED CONTEXT
- COMMENT ON TRUSTED CONTEXT
- CREATE TRUSTED CONTEXT
- DROP TRUSTED CONTEXT

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
ALTER TRUSTED CONTEXT				X
COMMENT ON TRUSTED CONTEXT	X		X	X
CREATE TRUSTED CONTEXT				X
DROP TRUSTED CONTEXT	X		X	X

7.3.4.19 View privileges

The following privileges are defined for views:

- COMMENT ON
- DELETE
- DROP
- INSERT
- INSTEAD OF TRIGGER
- REGENERATE VIEW
- SELECT
- UPDATE

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 in database class	SYSCTRL	SYSADM
COMMENT ON	X			X	X
DELETE		X			X
DROP	X			X	X
INSERT		X			X
INSTEAD OF TRIGGER	X			X	X
REGENERATE VIEW	X			X	X
SELECT		X			X
UPDATE		X			X

7.3.4.20 Specifics of discretionary access control when in Labeled Security Mode

The tables in sections 7.3.4.3 to 7.3.4.19 also list the implicit privileges of the owner of an object. Those privileges do not apply when the TOE is operated in Labeled Security Mode (AC.4-DB2-39).

7.3.5 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 Evaluated Configuration 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 Communication security in z/OS

As described above this security functionality is provided by the z/OS platform and described in the accordant chapter of [ZOSST].

7.5 Security management

7.5.1 Security management in z/OS

The security management of the z/OS platform is described in the [ZOSST].

7.5.2 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

RACF controlled access rights are managed using the RACF commands described in [ZOSST]. 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 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 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.

7.5.3 DB2 user attributes and user roles and database roles

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

- SYSADM
- Install SYSADM
- SYSCTRL
- SYSOPR
- Install SYSOPR
- DBADM
- DBCTRL
- DBMAINT
- PACKADM

SYSADM, SYSCTRL and SYSOPR are user roles with privileges on the DB2 subsystem level. 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 access³⁶ 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.

Figure 3 shows the hierarchy of user roles and the general privileges each user role has to DB2 objects.

³⁶ Sufficient access differs depending on whether the RACF MLS option is active or inactive:

- If the RACF MLS option is not active, a user with at least READ authorization to the resource has sufficient access.
- If the RACF MLS option is active and the request is not a write request, a user with at least READ authorization to the resource has sufficient access.
- If the RACF MLS option is active, and the request involves a write request, a user at least UPDATE authorization to the resource has sufficient access.

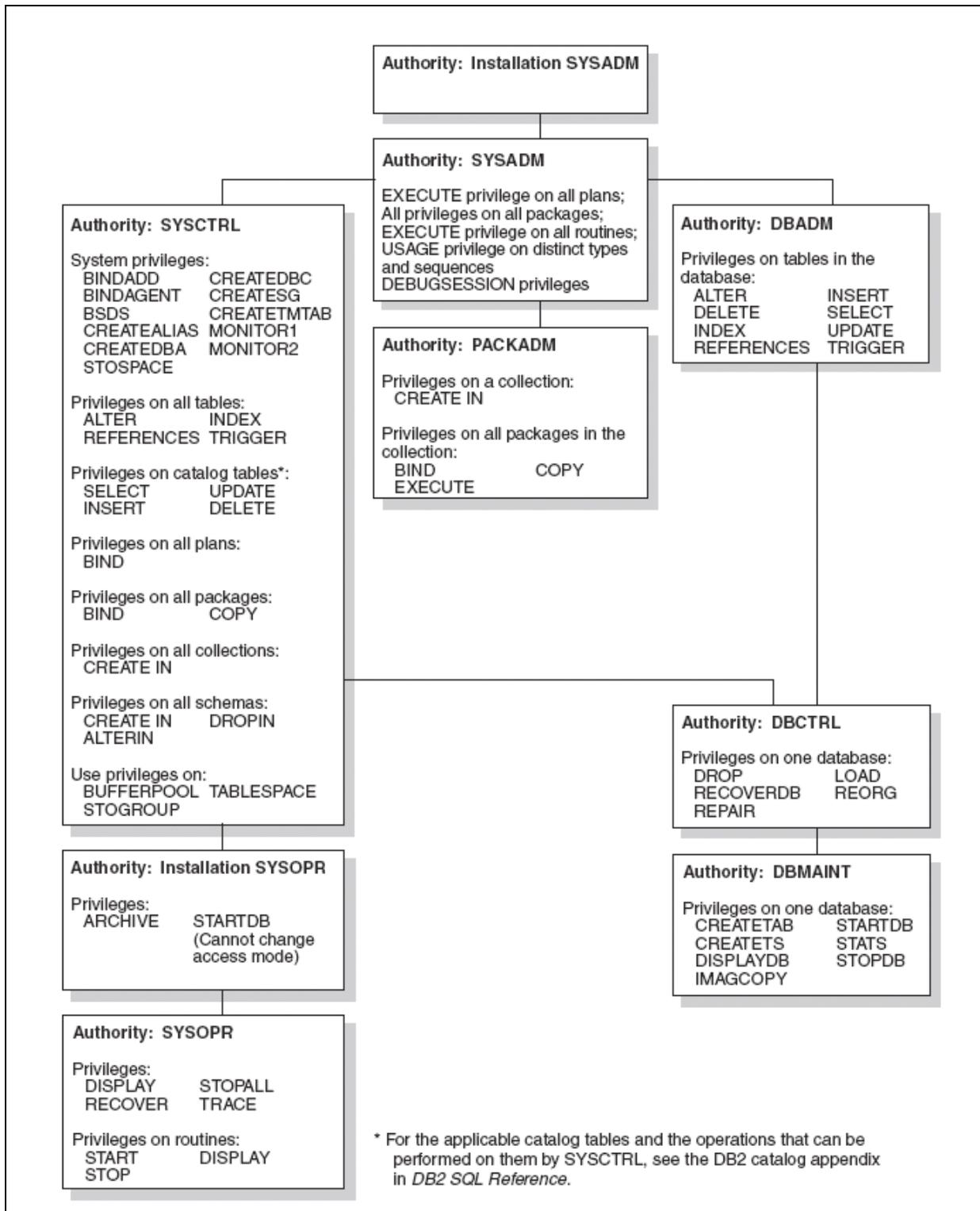


Figure 3: Hierarchy of user roles (administrative authorities) and their privileges in DB2

7.5.4 Trusted connections and database roles

Trusted connections allow the assignment of a different primary authorization ID, a database role or a security label 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 connections.

7.6 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].

7.6.1 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.

Audit class	Audit events that are traced
3	CREATE, ALTER, and DROP statements that affect audited tables, and the results of these statements. This class traces the dropping of a table that is caused by DROP TABLESPACE or DROP DATABASE and the creation of a table with AUDIT CHANGES or AUDIT ALL (AU.3-DB2-6).
4	<p>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.</p> <p>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).</p>
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).
6	<p>The bind of static and dynamic SQL statements of the following types:</p> <ul style="list-style-type: none"> • INSERT, UPDATE, DELETE, CREATE VIEW, and LOCK TABLE statements for audited tables. Except for the values of host variables, the audit record contains the first 4000 bytes of the 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 first 4000 bytes of the SQL statement (with record type IFCID 0350 included) (AU.3-DB2-10).
7	<p>Assignment or change of an authorization ID because of the following reasons (AU.3-DB2-11):</p> <ul style="list-style-type: none"> • 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 connection information and switch user information

Table 16: 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).

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).

7.7 Object reuse

7.7.1 Object reuse in z/OS

Please refer to the [ZOSST] for the object reuse functionality provided by the z/OS platform.

7.7.2 Object reuse in DB2

The trusted parts of DB2 execute in their own address spaces. Object reuse of memory objects within those address spaces is provided by the z/OS functions.

DB2 manages its own objects. When a DB2 object is deleted, DB2 ensures that the space that has been occupied by those objects can not 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 can not 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.

7.8 TOE self-protection

As described above this security functionality is provided by the z/OS platform and described in the accordant chapter of [ZOSST].

7.8.1 Protection of DB2 code and data structures

In addition DB2 executes as a z/OS subsystem using several address spaces. User programs can 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 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. This structure protects the DB2 code and internal data structures from unauthorized direct access by user programs.

DB2 objects are stored in z/OS data sets and those data sets need to be protected by RACF to prohibit unauthorized access by users. Users will need to call the DB2 functions to access the DB2 objects stored in those data sets and DB2 will check the user's access right to those objects before accessing it on behalf of the user. In the evaluated configuration DB2 will always invoke RACF to check for the user's access rights.

8 Abbreviations, Terminology and References

8.1 Abbreviations

APAR	Authorized Program Analysis Report
BSDS	Bootstrap Data Set
CAF	Call Attachment Facility
BR-DBMSPP	Basic Robustness Database Management System Protection Profile
CAPP	Controlled Access Protection Profile
CC	Common Criteria
DAC	Discretionary Access Control
DBRM	Data Base Request Module
DDM	Distributed Data Management
DFS	Data Facility Storage
DRDA	Distributed Relational Database Architecture
DSN	Data Source Name
ISPF	Interactivity System Product Facility
JAR	Java ARchive
LDAP	Lightweight Directory Access Protocol
LOB	Large Object in DB2
LSP	Labeled Security Protection Profile
MAC	Mandatory Access Control
MVS	Multiple Virtual Storage
PP	Protection Profile
PR/SM™	Processor Resource/Systems Manager™
RACF	Resource Access Control Facility
RRS	Resource Recovery Service
RRSAF	Resource Recovery Services Attachment Facility
SAF	System Authorization Facility
SDSF	System Display and Search Facility
SFR	Security Functional Requirement
SMF	System Management Facility
SNA	Systems Network Architecture
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

TSO	Time Sharing Option
TSP	TOE Security Policy

8.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] and [ZOSST] are not reiterated here, unless stated otherwise. This ST uses the following terms consistently with [CAPP] and [DBMSPP.BR]; they are described in this section to aid in the understanding by readers of this ST. Readers should be aware that some terms are used differently in other DB2 for z/OS documents. 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.

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).

Database

A set of DB2 structures that include 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 1.4.1.2 and 7.3.4.1 respectively.

DB2 subject

DB2 subjects are 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 1.4.1.1, 1.4.1.4, 7.3.4.2 and 7.5.4.

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 a 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.

Row

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

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

- [CC] Common Criteria for Information Technology Security Evaluation, Version 3.1R3, July 2009
Location <http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf>
Location <http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3.pdf>
Location <http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3.pdf>
- [CEM] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1R3, July 2009
Location <http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R3.pdf>
- [CAPP] Controlled Access Protection Profile, Version 1.d, Information Systems Security Organization. October 1999
- [DBMSPP.BR] U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments Version 1.2, July 2007
- [DB2AG] DB2 Version 9.1 for z/OS Administration Guide
Document Number: SC18-9840-03
Fourth Edition (December 2008)
- [DB2API] DB2 Version 9.1 for z/OS Application Programming and SQL Guide
Document Number: SC18-9841-03
Fourth Edition (December 2008)
- [DB2CR] DB2 Version 9.1 for z/OS Command Reference
Document Number: SC18-9844-03
Fourth Edition (December 2008)
- [DB2IG] DB2 Version 9.1 for z/OS Installation Guide
Document Number: GC18-9846-05
Sixth Edition (December 2008)
- [DB2INT] DB2 Version 9.1 for z/OS Introduction to DB2 for z/OS
Document Number: SC18-9847-02
Third Edition (December 2008)
- [DB2ACMG] DB2 Version 9.1 for z/OS RACF Access Control Module Guide
Document Number: SC18-9852-01
Second Edition (October 2007)
- [DB2WN] DB2 Version 9.1 for z/OS What's New
Document Number: GC18-9856-02
Third Edition (December 2008)

- [DB2SQL] DB2 Version 9.1 for z/OS SQL Reference
Document Number: SC18-9854-05
Sixth Edition (December 2008)
- [DB2UGR] DB2 Version 9.1 for z/OS Utility Guide and Reference
Document Number: SC18-9855-03
Fourth Edition (December 2008)
- [DRDA-V1] Open Group Technical Standard, DRDA Version 4 Vol. 1: Distributed Relational
Database Architecture
- [DRDA-V2] Open Group Technical Standard, DRDA Version 4 Vol. 2: Formatted Data Object
Content Architecture
- [DRDA-V3] Open Group Technical Standard, DRDA Version 4 Vol. 3: Distributed Data
Management Architecture
- [PMLS] Planning for Multilevel Security and the Common Criteria
Document Number: GA22-7509-08
Ninth Edition, April 2009
- [ZOSST] Security Target for IBM z/OS Version 1 Release 10
Version 5.11
March 2009

End of document