DB2 11 for z/OS Security Target

Version 1.9

Status: Final

Last Update: 2014-03-28

atsec is a trademark of atsec GmbH

IBM, IBM logo, DB2 11 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
- CPACF
- DFS
- @server
- IBM
- MVS
- PR/SM
- Print Services Facility
- RACF
- z/Architecture
- z/OS
- zSeries
- zEnterprise

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.

Document History

Version	Date	Summary	Author
1.9	2014-03-28	Version for public release	Alejandro Masino

Table of Content

1 Introduction ... 6
1.1 ST reference ... 6
1.2 TOE reference ... 6
1.3 TOE overview ... 6
1.4 TOE description ... 8
1.4.1 Structure of DB2 ... 8
1.4.2 TOE boundary and interfaces ... 13
1.4.3 Software security function summary ... 14
1.4.4 Configurations ... 16
2 Conformance claims ... 19
3 Security problem definition ... 20
3.1 Introduction ... 20
3.2 Threats ... 20
3.3 Organizational security policies ... 21
3.4 Assumptions ... 21
4 Security objectives ... 23
4.1 Security objectives for the TOE ... 23
4.2 Security objectives for the operational environment ... 24
4.3 Rationale for the Security Objectives ... 25
5 Extended components definition ... 26
6 Security requirements ... 27
6.1 TOE security functional requirements ... 27
6.1.1 Security audit (FAU) ... 33
6.1.2 User data protection (FDP) ... 36
6.1.3 Identification and authentication (FIA) ... 41
6.1.4 Security management (FMT) ... 42
6.1.5 Protection of the TSF (FPT) ... 44
6.2 Security Functional Requirements Rationale ... 45
6.2.1 Internal consistency and mutual support of SFRs ... 45
6.2.2 Coverage ... 47
6.2.3 Sufficiency ... 48
6.2.4 Security requirements dependency analysis ... 50
6.3 TOE security assurance requirements ... 51
6.4 Security Assurance Requirements Rationale ... 51
6.5 TOE Summary Specifications Rationale ... 52

6.5.1 Security functions justification 52
7 TOE summary specification 54
7.1 Overview of the TOE architecture 54
7.1.1 Main trusted subsystems of the evaluated configuration 55
7.2 Identification and authentication 56
7.2.1 Authentication function 56
7.2.2 Special handling in DB2 56
7.2.3 Trusted connections 56
7.3 Access control 57
7.3.1 Access control principles 57
7.3.2 Protected resources of DB2 57
7.3.3 Mandatory access control (Labeled Security Mode only) 58
7.3.4 Discretionary access control in DB2 59
7.3.5 DB2 internal access checking 75
7.3.6 Row and Column access control 75
7.4 Communication security in z/OS 76
7.5 Security management 76
7.5.1 Security management in z/OS 76
7.5.2 Security management of DB2 76
7.5.3 DB2 user attributes and user roles and database roles 77
7.5.4 Trusted connections and database roles 78
7.6 Auditing 78
7.6.1 Auditing in DB2 78
7.7 Object reuse 81
7.7.1 Object reuse in z/OS 81
7.7.2 Object reuse in DB2 81
7.8 TOE self-protection 81
7.8.1 Protection of DB2 code and data structures 81
8 Abbreviations, Terminology and References 83
8.1 Abbreviations 83
8.2 Terminology 84
8.3 References 86

1 Introduction

1.1 ST reference

Title:	DB2 11 for z/OS Security Target
Version:	1.9
Status:	Final
Date:	2014-03-28
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 11 for z/OS Version 1 Release 13.

1.3 TOE overview

The Target of Evaluation (TOE) consists of:

- The “IBM z/OS Version 1 Release 13 (z/OS V1R13)” operating system, including the Resource Access Control Facility (RACF) which is used as the evaluated platform.
- The “IBM DB2 11 for z/OS” (DB2 11), which is built upon this platform.

This Security Target (ST) builds on the z/OS Security Target [ZOSST], which refers to the “IBM z/OS Version 1 Release 13” operating system, evaluated under certificate ID BSI-DSZ-CC-0788-2012 (see [BSI-zOS] for more information).

DB2 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 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 V1R13 security target where the additional security functionality of DB2 is described. To avoid redundancy with the z/OS security target, this document only describes the additional or modified security functionality introduced by DB2.

DB2 is a component that uses and extends the functionality of z/OS V1R13. This evaluation is based on the evaluation of the z/OS V1R13 itself and will therefore only claim security functionality provided by DB2.

The z/OS Security Target [ZOSST] contains, in section 1.3 “TOE overview”, an introduction about the z/OS V1R13 operating system 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 the IBM, System z® platform.

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

DB2 for z/OS provides security options for e-business and high security with multilevel security, row-level and column level security as well as high security, more granularity and more information for additional flexibility in applications and SQL, and encryption capabilities. Notice that cryptography is not claimed as security functionality in this ST.

In addition DB2 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.

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). 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 cannot be altered by a user unless he has the specific privilege to overwrite labels. This column cannot be dropped from the table.

The TOE also provides accountability through the generation of audit records provided by both the z/OS platform and DB2.The TOE also allows the use of audit policies to configure the level and scope of the audit functionality.

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

In this ST, the TOE consists of one instance of z/OS V1R13 running on an abstract machine as the sole operating system exercising full control over it, and DB2 running on top of z/OS V1R13.

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 V1R13 (see [ZOSST]), DB2 relies on the mechanisms provided by the underlying operating system.

The required runtime environment for the z/OS V1R13 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.

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 V1R13 and DB2 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 standard 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 11 for z/OS (DB2) on the IBM z/OS Version 1 Release 13 (z/OS V1R13) operating system, including the Resource Access Control Facility (RACF).

The security description and configuration of the z/OS V1R13 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 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.

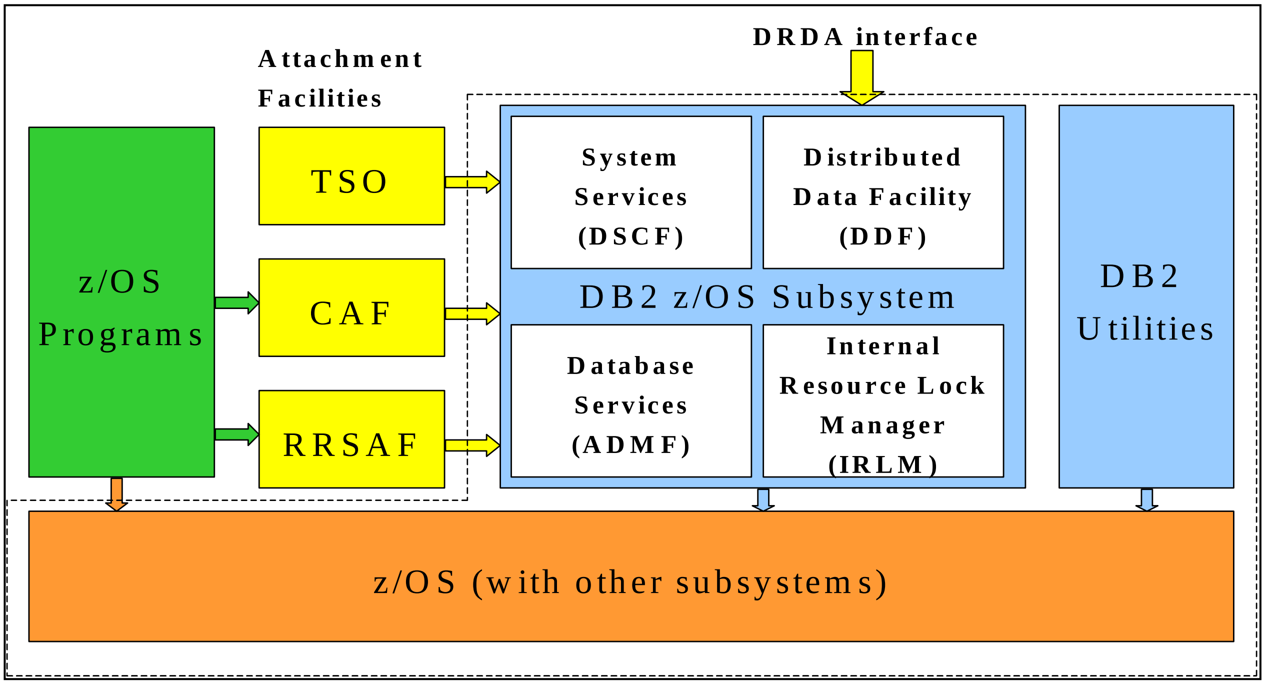

Figure 1: Basic structure of DB2 for z/OS showing TOE structure with TOE boundary

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 V1R13 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 discretionary 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.

DB2 also enforces access control at table row and column levels.

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
  - User-defined type – not in evaluated configuration
  - Sequence
  - Row permission
  - Column mask
- Trusted context
- Global variable

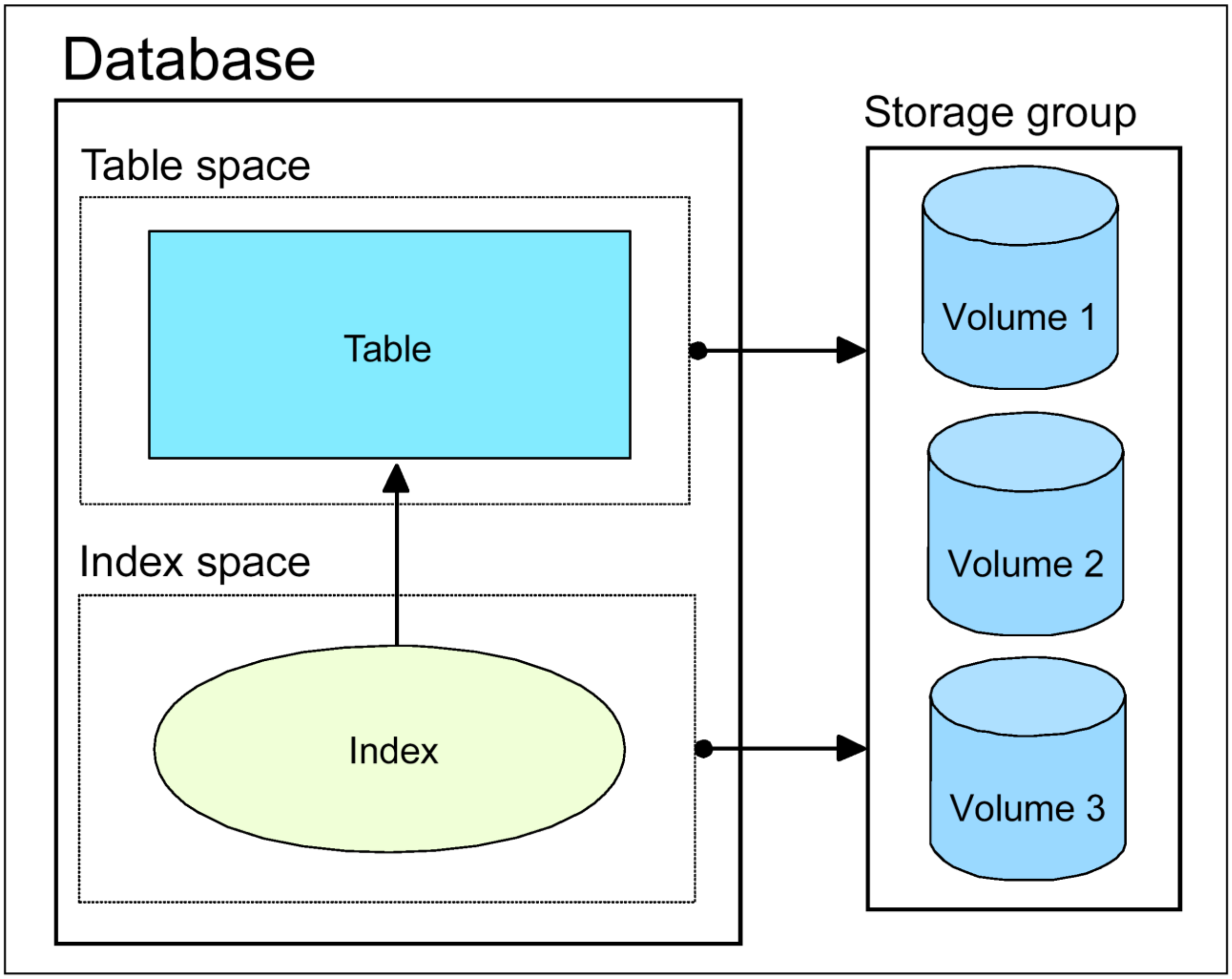

Figure 2: (Simplified) structure of a DB2 database

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

Privileges

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

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

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

Administrative Authority

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

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

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

System authorities include:

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

- SYSCTRL: System control authority includes most SYSADM privileges; it excludes the privileges to read or change user data. In case the SEPARATE_SECURITY system parameter is set to NO, SYSCTRL can also create roles.
- SYSOPR: System operator authority includes the privileges to issue most DB2 commands and end any utility job.
- SECADM: Security administration authority that manages security related objects (row permissions, column masks, roles, trusted contexts, secured triggers and user-defined functions), creates audit policies, and grant and revoke privileges and authorities (not allowed in the evaluated configuration).
- System DBADM or SYSDBADM: Database administration authority that allows the separation of object management from data access and granting of privileges. System DBADM can manage databases across a DB2 subsystem (i.e. create, alter and drop DB2 objects), while having no access to the data in the databases.
- SQLADM: SQL administration authority provides the ability to monitor and tune SQL without any additional privileges.
- DATAACCESS: Data access administrative authority that can access data in all user tables.
- ACCESSCTRL: Access control administrative authority that does grants and revokes (not allowed in the evaluated configuration).

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

- Install SYSADM
- Install SYSOPR

Database authorities (ranked from highest to lowest) include:

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

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

Collection authorities include:

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

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

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

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 11 for z/OS and z/OS Version 1 Release 13.

z/OS Version 1 Release 13 (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 user role (DB2 administrative authority), or has access based on the access right he has been assigned in the access list of the profile protecting the authority to the resource (DB2 explicit privilege). Depending on the type of object and the authority requested he may also use the authority when he is the owner of the object (DB2 implicit privilege).

DB2 also allows object ownership by database roles. A database role can own database objects, which helps eliminate the need for individual users to own and control database objects; instead, the database role is then assigned to an individual user or a group of users thus offering a mechanism other than authorization IDs through which privileges and authorities can be assigned. Database roles are applicable in a trusted context: a database entity based on a system authorization ID and a set of connection trust attributes.

DB2 also allows the enforcement of access control on tables at row and column levels through filtering and data masking:

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

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

1.4.3.3 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. The column used as a security label cannot be dropped from the table.

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.

DB2 also allows the configuration of the audit functionality based on audit policies.

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 V11 Package, which includes:
    - One of the two versions of DB2 11 for z/OS:
        - the standard DB2 11 for z/OS (program number 5615-DB2)
        - DB2 11 for z/OS VUE (value unit edition) (program number 5697-P43), which delivers a one-time-charge price metric for Eligible Workloads.
    - DB2 Utilities Suite for z/OS, V11 (program number 5655-W87)
- The Common Criteria Evaluated Base for z/OS V1R13 Package (certificate ID BSI-DSZ-CC-0788-2012), as specified in the Security Target for IBM z/OS Version 1 Release 13 ([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 1.4.3.1.

Both versions of DB2 11 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 11 for z/OS VUE license.

In case the licensing option is chosen, DB2 11 for z/OS VUE requires running in a logical partition (LPAR) on z/OS V1R13 configured as zNALC (System z New Application License Charges).

For the purpose of this evaluation, DB2 11 for z/OS(program number 5615-DB2) will be used.

Additionally, both versions of DB2 11 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:

•	HIYBB10	IMS Attach
•	JDBBB12	JDBC/SQLJ
•	JDBBB17	ODBC
•	JDBBB1X	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 1.4.3.1.

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 HIYBB10)
- Java Archives (JAR)
- JDBC/SQLJ (FMID JDBBB12)
- Kerberos
- ODBC/CLI (FMID JDBBB17)
- PassTickets
- Secondary authorization IDs
- Sign-on authorization IDs
- SNA™ connections
- Unified debugger
- XML Extender (FMID JDBBB1X)
- 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.

To operate the TOE in either the standard mode or Labeled Security mode of operation, the product 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: “DB2 11 for z/OS Common Criteria Guide” [DB2CCG] and “DB2 11 for z/OS Administration Guide" [DB2AG]. Also refer to the DB2 guidance for more information about protection panel fields and acceptable values in the evaluated configuration.

1.4.4.2 Hardware configurations

This TOE allows the use of all hardware and hardware configurations as defined in [ZOSST], section 1.4.3.2. The TOE is running within a logical partition provided by a certified version of PR/SM, on the z/Architecture as implemented by the following hardware platforms:

- IBM System z10 Business Class with CP Assist for Cryptographic Functions (CPACF) DES/TDES Enablement Feature 3863 active, optionally with CryptoExpress3 card.
- IBM System z10 Enterprise Class with CPACF DES/TDES Enablement Feature 3863 active, optionally with CryptoExpress3 card.

- IBM zEnterprise 114 with CPACF DES/TDES Enablement Feature 3863 active , optionally with CryptoExpress3 card, and with or without the zEnterprise BladeCenter Extension (zBX).
- IBM zEnterprise 196 with CPACF DES/TDES Enablement Feature 3863 active, optionally with CryptoExpress3 card, and with or without the zEnterprise BladeCenter Extension (zBX).

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

The following peripherals can be used with the TOE, while still preserving the security functionality:

- All terminals that are supported by the TOE.
- Printers:
  - in standard operation mode: any printer that is supported by the TOE.
  - in Labeled Security Mode: any printer that is used to print output with different security labels must support the Guaranteed Print Labeling Function. Guaranteed print labeling works with a subset of Advanced Function Presentation™ (AFP™) printers and ensures the integrity of the identification label by preventing the user from changing the label. Review the printer hardware documentation or contact the printer vendor to determine if a printer supports this function.
- All storage devices and backup devices supported by the TOE, such as:
  - Direct access storage devices (DASDs), except RVA devices.
- Tape drives (including encrypting tape drives, though this evaluation has not specifically examined those cryptographic functions).
  - All Ethernet and token-ring network adapters that are supported by the TOE.

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 11 for z/OS Common Criteria Guide (SC19-4011-00)
- DB2 11 for z/OS What's New? (GC19-4068-00)
- DB2 11 for z/OS Introduction to DB2 for z/OS (SC19-4058-00-EB)
- DB2 11 for z/OS Installation Guide (GC19-4056-00)
- DB2 11 for z/OS Administration Guide (SC19-4050-00)
- DB2 11 for z/OS Command Reference (SC19-4054-00)DB2 11 for z/OS Manage Security Guide (SC19-4061-EB)
- DB2 11 for z/OS RACF Access Control Module Guide (SC19-4065-00)
- DB2 11 for z/OS Data Sharing: Planning and Administration (SC19-4055-00)
- DB2 11 for z/OS Codes (GC19-4053-01)
- DB2 11 for z/OS Messages (GC19-4062-01)
- DB2 11 for z/OS Application Programming Guide and Reference for Java™ (SC19-4052-00)
- DB2 11 for z/OS Application Programming and SQL Guide (SC19-4051-00)
- DB2 11 for z/OS SQL Reference (SC19-4066-00)
- DB2 11 for z/OS Utility Guide and Reference (SC19-4067-EB)
- DB2 11 for z/OS Diagnosis Guide and Reference (LY37-3222-00)

2 Conformance claims

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 revision 4 has been taken as the basis for this conformance claim.

This Security Target makes claims on the following protection profile and extended packages:

- [OSPP]: Operating System Protection Profile. Version 2.0 as of 2010-06-01; ***strict conformance***.
- [OSPP-EIA]: OSPP - Identification and Authentication extended package ***conformant***. Version 2.0 as of 2010-05-28.
- [OSPP-LS]: OSPP - Labeled Security extended package ***conformant***. Version 2.0 as of 2010-05-28.

This protection profile and its extended packages are listed on the BSI web site as validated profiles (certification ID BSI-CC-PP-0067-2010). See [BSI-PP] for more information.

3 Security problem definition

3.1 Introduction

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

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

This Security Target claims conformance to the Operating System Protection Profile base [OSPP], as well as its extended packages for extended identification and authentication [OSPP-EIA], and labeled security [OSPP-LS]. The Assets, Assumptions, Threats and Organizational Security Policies of this Protection Profile 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 section 3.2.3 “Threats countered by the TOE” of the z/OS Security Target [ZOSST]. There are no additional threats defined in this ST.

The following table shows the threats defined in [ZOSST]:

Name	Definition
T.ACCESS.TSFDATA	A threat agent might read or modify TSF data without the necessary authorization when the data is stored or transmitted.
T.ACCESS.USERDATA	A threat agent might use or modify functionality of the TSF without the necessary privilege to grant itself or others unauthorized access to TSF data or user data.
T.ACCESS.TSFFUNC	A threat agent might use or modify functionality of the TSF without the necessary privilege to grant itself or others unauthorized access to TSF data or user data. A threat agent might use or modify functionality of the TSF without the necessary privilege to grant itself or others unauthorized access to TSF data or user data.
T.ACCESS.COMM	A threat agent might access a communication channel that establishes a trust relationship between the TOE and another remote trusted IT system or masquerade as another remote trusted IT system.
T.RESTRICT.NETTRAFFIC	A threat agent might get access to information or transmit information to other recipients via network communication channels without authorization for this communication attempt by the information flow control policy.
T.IA.MASQUERADE	A threat agent might masquerade as an authorized entity including the TOE itself or a part of the TOE in order to gain unauthorized access to user data, TSF data, or TOE resources.
T.IA.USER	A threat agent might gain access to user data, TSF data or TOE resources with the exception of public objects without being identified and authenticated.

Name	Definition
T.DATA_NOT_SEPARATED	The TOE may not adequately separate data on the basis of its sensitivity label, thereby allowing information to flow illicitly from or to users.

Table 1 - Threats

3.3 Organizational security policies

This Security Target includes all Organizational Security Policies defined in section 3.4 “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 [ZOSST]:

Name	Defined in
P.ACCOUNTABILITY	The users of the TOE shall be held accountable for their security-relevant actions within the TOE.
P.USER	Authority shall only be given to users who are trusted to perform the actions correctly.
P.I&A.REMOTE	Remote trusted IT systems shall be able to obtain identification and authentication decisions from the TOE based on credentials transmitted by a remote trusted IT system to the TOE.
P.CLEARANCE	The system must limit the information flow between protected resources and authorized users based on whether the user's sensitivity label is appropriate for the labeled information.
P.LABELED_OUTPUT	The beginning and end of all paged, hardcopy output must be marked with sensitivity labels that properly represent the sensitivity label of the output.
P.RESOURCE_LABELS	All resources accessible by subjects and all subjects must have associated labels identifying the sensitivity levels of data contained therein.
P.USER_CLEARANCE	All users must have a clearance level identifying the maximum sensitivity levels of data they may access.

Table 2 - Organizational security policies

3.4 Assumptions

This Security Target includes all assumptions defined in section 3.3 “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 [ZOSST]:

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

Name	Definition
A.MANAGE	The TOE security functionality is managed by one or more competent individuals. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.
A.AUTHUSER	Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.
A.TRAINEDUSER	Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.
A.DETECT	Any modification or corruption of security-enforcing or security-relevant files of the TOE, user or the underlying platform caused either intentionally or accidentally will be detected by an administrative user.
A.PEER.MGT	All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to be under the same management control and operate under security policy constraints compatible with those of the TOE.
A.PEER.FUNC	All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality.
A.CONNECT	All connections to and from remote trusted IT systems and between physically-separate parts of the TSF not protected by the TSF itself are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.

Table 3 - Assumptions

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 [[ZOSST], all of which are applicable to the security problem definition:

Name	Definition
O.AUDITING	The TSF must be able to record defined security-relevant events (which usually include security-critical actions of users of the TOE). The TSF must protect this information and present it to authorized users if the audit trail is stored on the local system. The information recorded for security-relevant events must contain the time and date the event happened and, if possible, the identification of the user that caused the event, and must be in sufficient detail to help the authorized user detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.
O.CRYPTO.NET	The TSF must allow authorized users to remotely access the TOE using a cryptographically-protected network protocol that ensures integrity and confidentiality of the transported data and is able to authenticate the end points of the communication. Note that the same protocols may also be used in the case where the TSF is physically separated into multiple parts that must communicate securely with each other over untrusted network connections.
O.DISCRETIONARY.ACCESS	The TSF must control access of subjects and/or users to named resources based on identity of the object. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.
O.NETWORK.FLOW	The TOE shall mediate communication between sets of TOE network interfaces, between a network interface and the TOE itself, and between subjects in the TOE and the TOE itself in accordance with its security policy.
O.SUBJECT.COM	The TOE shall mediate communication between subjects acting with different subject security attributes in accordance with its security policy.
O.I&A	The TOE must ensure that users have been successfully authenticated before allowing any action the TOE has defined to provide to authenticated users only.
O.MANAGE	The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms and must ensure that only authorized users are able to access such functionality.

Name	Definition
O.TRUSTED_CHANNEL	The TSF must be designed and implemented in a manner that allows for establishing a trusted channel between the TOE and a remote trusted IT system that protects the user data and TSF data transferred over this channel from disclosure and undetected modification and prevents masquerading of the remote trusted IT system.
O.I&A.REMOTE	The TOE shall allow remote trusted IT systems to transmit user credentials to the TOE which are used to perform a local identification and authentication policy decision. This decision is communicated back to one or more remote trusted IT systems based on the identification and authentication policy.
O.I&A.MULTIPLE	The TOE shall allow the concurrent use of multiple identification and authentication mechanisms implementing the identification and authentication policy.
O.LS.CONFIDENTIALITY	The TOE will control information flow between entities and resources based upon the sensitivity labels of users and resources.
O.LS.PRINT	The TOE will provide the capability to mark printed output with accurate labels based on the sensitivity label of the user causing the output.
O.LS.LABEL	The TOE will provide the capability to label all subjects, and all objects accessible by subjects, to restrict information flow based on the sensitivity labels.
O.CRYPTO.BASIC	The TSF will provide the following cryptographic services for general use by authorized entities, using support from the underlying platform: • symmetric and asymmetric ciphers • message digest generation • symmetric and asymmetric key generation

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 [ZOSST].

Name	Definition
OE.ADMIN	Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
OE.REMOTE	If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide the functions required by the TOE and are sufficiently protected from any attack that may cause those functions to provide false results.
OE.INFO_PROTECT	Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate

Name	Definition
	manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data held by the system. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted. • DAC protections on security-relevant files (such as audit trails and authentication databases) shall always be set up correctly. Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.
OE.INSTALL	Those responsible for the TOE must establish and implement procedures to ensure that the hardware, software and firmware components that comprise the system are distributed, installed and configured in a secure manner supporting the security mechanisms provided by the TOE.
OE.MAINTENANCE	Authorized users of the TOE must ensure that the comprehensive diagnostics facilities provided by the product are invoked at every scheduled preventative maintenance period.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.
OE.RECOVER	Those responsible for the TOE must ensure that procedures and/or mechanisms are provided to assure that after system failure or other discontinuity, recovery without a protection (security) compromise is achieved.
OE.TRUSTED.IT.SYSTEM	The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are under the same management domain as the TOE, are managed based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.

Table 5 - Security objectives for the Operational Environment

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]. 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.

5 Extended components definition

This ST does not define extended components; only the extensions defined in [OSPP], [OSPP-EIA] and [ZOSST] are used:

- [OSPP] defines three extended components:
    - FCS_RNG.1: Random number generation.
    - FDP_RIP.3: Full residual information protection of subjects.
    - FIA_USB.2: Enhanced user-subject binding.
- [OSPP-EIA] defines two extended components:
    - FIA_UAU.8: Authentication policy decisions.
    - FIA_UID.3: Identification policy decisions.
- [ZOSST] defines two extended components:
    - FCS_COP_EXT.1: Cryptographic operation with platform support.
    - FCS_CKM_EXT.1: Cryptographic key generation with platform support.

6 Security requirements

6.1 TOE security functional requirements

This section defines the functional requirements for the TOE. Functional requirement components in this Security Target were drawn from the Operating System Protection Profile base and its extensions ([OSPP], [OSPP-EIA] and [OSPP-LS]), the extended security functional components defined in [ZOSST] 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. This ST adopts the following convention for operations performed on security functional components:

- Operations already performed in [OSPP] and its extensions are kept without any special formatting.
- Refinement operations are marked in bold, italic and underlined text.
- Assignment and selection operations are marked in bold text.

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 standard modes of operation.

To support a better understanding of the combination Security Target of the z/OS platform [ZOSST] vs. this DB2 Security Target, the following table 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
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	Protected audit trail storage
FAU_STG.3	Action in case of possible audit data loss
FAU_STG.4	Prevention of audit data loss
FCS_CKM.1(SYM)	Cryptographic key generation: symmetric algorithms
FCS_CKM.1(RSA)	Cryptographic key generation: RSA
FCS_CKM.1(DSA)	Cryptographic key generation: DSA
FCS_CKM_EXT.1(ECDSA)	Cryptographic key generation: ECDSA
FCS_CKM.2(NET)	Cryptographic key distribution
FCS_CKM.4	Cryptographic key destruction
FCS_COP_EXT.1(SGN)	Cryptographic operation: signatures
FCS_COP.1(NET)	Cryptographic operation: network
FCS_COP_EXT.1(CRYPTO-ENC)	Cryptographic operation: general purpose encryption/decryption
FCS_COP_EXT.1(CRYPTO-MD)	Cryptographic operation: general purpose message digest generation

Name	Title
FCS_COP_EXT.1(CRYPTO-SGN)	Cryptographic operation: general purpose signature generation and verification
FCS_RNG.1	Random number generation
FDP_ACC.1(PSO)	Subset access control: persistent objects
FDP_ACC.1(TSO)	Subset access control: transient objects
FDP_ACF.1(PSO-MVS)	Security attribute based access control: MVS
FDP_ACF.1(PSO-UNIX)	Security attribute based access control: UNIX
FDP_ACF.1(PSO-LDAP)	Security attribute based access control: LDAP
FDP_ACF.1(TSO)	Security attribute based access control: UNIX IPC
FDP_ETC.1 (Labeled Security Mode only)	Export of user data without security attributes
FDP_ETC.2(LS) (Labeled Security Mode only)	Export of user data with security attributes
FDP_IFC.2(LS) (Labeled Security Mode only)	Complete information flow control: labeled security
FDP_IFC.2(NI)	Complete information flow control: network
FDP_IFF.1(NI)	Simple security attributes
FDP_IFF.2(LS) (Labeled Security Mode only)	Hierarchical security attributes
FDP_ITC.1(LS) (Labeled Security Mode only)	Import of user data without security attributes
FDP_ITC.2	Import of user data with security attributes
FDP_ITC.2(LS) (Labeled Security Mode only)	Import of user data with security attributes: labeled security
FDP_RIP.2	Full residual information protection
FDP_RIP.3	Full residual information protection of resources
FIA_AFL.1	Authentication failure handling
FIA_ATD.1(HU)	User attribute definition: human users
FIA_ATD.1(TU)	User attribute definition: technical users
FIA_ATD.1(EIA)	User attribute definition: EIA
FIA_ATD.1(LS) (Labeled Security Mode only)	User attribute definition: labeled security
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.7	Protected authentication feedback
FIA_UAU.8(EIA)	Authentication policy decisions
FIA_UID.1	Timing of identification
FIA_UID.3(EIA)	Identification policy decisions
FIA_USB.1(LS) (Labeled Security Mode only)	User-subject binding
FIA_USB.2	Enhanced user-subject binding
FMT_MSA.1(PSO)	Management of object security attributes: persistent objects

Name	Title
FMT_MSA.1(TSO)	Management of object security attributes: transient objects
FMT_MSA.1(LS) (Labeled Security Mode only)	Management of object security attributes: labeled security
FMT_MSA.3(PSO)	Static attribute initialization: persistent objects
FMT_MSA.3(TSO)	Static attribute initialization: transient objects
FMT_MSA.3(NI)	Static attribute initialization: network
FMT_MSA.3(LS) (Labeled Security Mode only)	Static attribute initialization: labeled security
FMT_MSA.4(PSO)	Security attribute value inheritance: persistent objects
FMT_MTD.1(AE)	Management of TSF data: audit events
FMT_MTD.1(AS)	Management of TSF data: audit storage
FMT_MTD.1(AT)	Management of TSF data: audit trail threshold
FMT_MTD.1(AF)	Management of TSF data: audit storage failure
FMT_MTD.1(NI)	Management of TSF data: network filters
FMT_MTD.1(NI2)	Management of TSF data: IPSec
FMT_MTD.1(IAT)	Management of TSF data: authentication threshold
FMT_MTD.1(IAF)	Management of TSF data: account re-enablement
FMT_MTD.1(IAU)	Management of TSF data: user security attributes
FMT_MTD.1(IAU-AUTH)	Management of TSF data: authentication data
FMT_MTD.1(EIA)	Management of TSF data: EIA
FMT_MTD.1(CRYPTO1)	Management of TSF data: key import
FMT_MTD.1(CRYPTO2)	Management of TSF data: digital certificates
FMT_MTD.1(ADD)	Management of TSF data: additional configuration
FMT_REV.1(OBJ)	Revocation: objects
FMT_REV.1(USR)	Revocation: users
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_STM.1	Reliable time stamps
FPT_TDC.1	Inter-TSF basic TSF data consistency
FPT_TDC.1(LS) (Labeled Security Mode only)	Inter-TSF basic TSF data consistency: labeled security
FTA_SSL.1	TSF-initiated session locking
FTA_SSL.2	User-initiated locking
FTP_ITC.1	Inter-TSF trusted channel

Table 6 - Security Functional Requirements for the z/OS platform

The table below lists the Security Functional Requirements (SFR) defined in this Security Target. Each row describes an SFR, where it was originally defined ([OSPP] and their extensions, [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 this ST. See [ZOSST] for the definition of those SFRs.

Name	Title	Defined by			Enforced by	
		OSPP	CC Part 2	z/OS ST	z/OS	DB2
FAU_GEN.1(DB2)	Audit data generation	✓			✓	✓
FAU_GEN.2	User identity association			✓	✓	✓
FAU_SEL.1(DB2)	Selective audit	✓			✓	✓
FDP_ACC.2(DB2)	Discretionary access control policy in DB2		✓			✓
FDP_ACF.1(DB2)	Discretionary access control functions for DB2 objects		✓			✓
FDP_ACC.1(RCAC)	Complete access control policy on DB2 rows and columns		✓			✓
FDP_ACF.1(RCAC)	Security attribute based access control on DB2 rows and columns.		✓			✓
FDP_ETC.1	Export of user data without security attributes (Labeled Security Mode only)			✓	✓	✓
FDP_ETC.2(LS)	Export of user data with security attributes (Labeled Security Mode only)			✓	✓	✓
FDP_IFC.2(LS-DB2)	Complete information flow control in DB2 (Labeled Security Mode only)	✓				✓
FDP_IFF.2(LS)	Hierarchical security attributes (Labeled Security Mode only)			✓	✓	✓
FDP_ITC.1(LS)	Import of user data without security attributes (Labeled Security Mode only)			✓	✓	✓
FDP_ITC.2	Import of user data with security attributes			✓	✓	✓
FDP_ITC.2(LS)	Import of user data with security attributes: labeled security (Labeled Security Mode only)			✓	✓	✓
FDP_RIP.2	Full residual information protection			✓	✓	✓
FDP_RIP.3	Full residual information protection of resources			✓	✓	✓
FIA_ATD.1(DB2)	User attribute definition		✓			✓
FIA_UAU.2(DB2)	User authentication before any action in DB2		✓			✓
FIA_UID.2(DB2)	User identification before any action in DB2		✓			✓
FIA_USB.1(DB2)	User-subject binding		✓			✓
FMT_MSA.1(DB2)	Management of security attributes in DB2		✓			✓
FMT_MSA.1(LS-DB2)	Management of object security attributes for DB2 rows (Labeled Security Mode only)		✓			✓
FMT_MSA.3(DB2)	Static attribute initialization in DB2		✓			✓
FMT_MSA.3(LS-DB2)	Static attribute initialization for rows in DB2 tables and MAC (Labeled Security Mode only)		✓			✓
FMT_MTD.1(AE-DB2)	Management of TSF data: audit events		✓			✓
FMT_SMF.1(DB2)	Specification of management functions		✓			✓
FMT_SMR.1(DB2)	Security roles		✓			✓
FPT_TDC.1(LS-DB2)	Inter-TSF basic TSF data consistency (Labeled		✓			✓

Name	Title	Defined by			Enforced by	
		OSPP	CC Part 2	z/OS ST	z/OS	DB2
	Security Mode only)					

Table 7 - 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(LS)	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.

Table 8: DB2 Application Notes for SFRs

SFR	OSPP					z/OS ST	CC Part 2					Comments
	D	A	S	R	I		D	A	S	R	I	
FAU_GEN.1(DB2)	✓			✓	✓							
FAU_GEN.2						✓						Not repeated in this ST.
FAU_SEL.1(DB2)	✓			✓	✓							
FDP_ACC.2(DB2)							✓	✓			✓	
FDP_ACF.1(DB2)							✓	✓		✓	✓	
FDP_ACC.1(RCAC)							✓	✓			✓	
FDP_ACF.1(RCAC)							✓	✓			✓	
FDP_ETC.1						✓						Not repeated in this ST.
FDP_ETC.2(LS)						✓						Not repeated in this ST, added application note.
FDP_IFC.2(LS-DB2)	✓	✓		✓	✓							
FDP_IFF.2(LS)						✓						Not repeated in this ST.
FDP_ITC.1(LS)						✓						Not repeated in this ST.
FDP_ITC.2						✓						Not repeated in this ST.
FDP_ITC.2(LS)						✓						Not repeated in this ST.
FDP_RIP.2						✓						Not repeated in this ST.
FDP_RIP.3						✓						Not repeated in this ST.
FIA_ATD.1(DB2)							✓	✓		✓	✓	
FIA_UAU.2(DB2)							✓	✓			✓	
FIA_UID.2(DB2)							✓	✓			✓	
FIA_USB.1(DB2)							✓	✓			✓	
FMT_MSA.1(DB2)							✓	✓		✓	✓	
FMT_MSA.1(LS-DB2)							✓	✓		✓	✓	

SFR	OSPP					z/OS ST	CC Part 2					Comments
	D	A	S	R	I		D	A	S	R	I	
FMT_MSA.3(DB2)							✓	✓		✓	✓	
FMT_MSA.3(LS-DB2)							✓	✓		✓	✓	
FMT_MTD.1(AE-DB2)							✓	✓			✓	
FMT_SMF.1(DB2)							✓	✓			✓	
FMT_SMR.1(DB2)							✓	✓			✓	
FPT_TDC.1(LS-DB2)							✓	✓			✓	

Table 9 - Operations performed in SFRs

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

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; and

c) all modifications to the set of events being audited;

d) all user authentication attempts;

e) all denied accesses to objects for which the access control policies defined in ~~***the OSPP base***~~ ***this ST*** applies;

f) explicit modifications of access rights to objects covered by the access control policies; and

g) **the events listed in *Table 10: DB2 auditable events.***

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST:

i. User identity (if applicable); and

ii. (in Labeled Security Mode) The sensitivity labels of subjects, objects, or information involved; and

iii. The additional information specified in the "Details" column *of Table 10: 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.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.2(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(LS) (Labeled Security mode)	All attempts to export information.	SMF type 80 record, event code 2, for TAPEVOL class. (see Note 2)
FDP_ETC.2(LS) (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.2(LS-DB2) (Labeled Security mode)	None.	
FDP_IFF.2(LS) (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(LS) (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(LS) (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.	
FDP_RIP.3	None.	
FIA_ATD.1(DB2)	None.	
FIA_UAU.2(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.2(DB2)	All use of the user identification mechanism, including the identity provided *during successful attempts*.	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)

Security Functional Requirement	Auditable Event(s)	Details
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_MSA.1(DB2)	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(LS-DB2)	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.3(DB2)	None	
FMT_MSA.3(LS-DB2)	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(AE-DB2)	All modifications to the values of TSF data.	SMF type 80 record (generated by the RACF commands). Covered by z/OS/RACF.
FMT_SMF.1(DB2)	None specifically associated with this SFR, but auditing is covered under the FMT_MSA.1(DB2), FMT_MSA.1(LS-DB2), FMT_MSA.3(DB2), FMT_MSA.3(LS-DB2), FMT_MTD.1(AE-DB2), FMT_REV.1, FAU_SAR.1, FAU_SEL.1, FAU_STG.3, FAU_STG.4, and FMT_SMR.1(DB2) 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(LS-DB2)	None	

Table 10: 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 Selective audit (FAU_SEL.1(DB2))

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

a) Type of audit event***;***

b) ~~***Subject or***~~ user identity***;***

c) Outcome (success or failure) of the audit event;

d) Named object identity***;***

e) Subject sensitivity label; (Labeled Security Mode only)

f) Object sensitivity label; (Labeled Security Mode only)

g) Audit level for table name;

h) Audit policy, consisting of:

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

6.1.2 User data protection (FDP)

6.1.2.1 Discretionary access control policy *in DB2* (FDP_ACC.2(DB2))

FDP_ACC.2.1 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, trusted contexts, row**

permissions, column masks and global variables) and all operations among subjects and objects covered by the SFP.

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 following access control attributes associated with a DB2 subject:**

- **User identity**
- **The primary authorization ID of the user.**
- **Group membership(s)**
- **The TRUSTED and PRIVILEGE attributes.**
- **The user role(s) (administration authorities) of the user.**

b) **The following access control attributes associated with a DB2 object:**

- **The user's access right in the RACF access control list for the RACF profile protecting the DB2 authority (privilege) the user is using to access the object.**
- **The ownership (by a user or database role) of the DB2 object.**

c) **The trusted connection established by a DB2 subject and the following access control attributes associated with the related trusted context:**

- **The database role(s).**

d) **The privilege or administration authority needed to perform the operation on the DB2 object.**

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 to an operation on a DB2 object if

- **the privilege 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 privilege 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 privilege 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 privilege 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 privilege 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 privilege 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 posses 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(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.**

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

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

6.1.2.3 Subset access control on *DB2 rows and columns* (FDP_ACC.1(RCAC))

FDP_ACC.1.1 The TSF shall enforce the **Row and Column Access Control Policy** on

a) **Subjects: DB2 processes acting on behalf of users;**

b) **Objects: table rows and table columns**

c) **Operations: SELECT, INSERT, UPDATE, DELETE.**

6.1.2.4 Security attribute based access control on *DB2 rows and columns* (FDP_ACF.1(RCAC))

FDP_ACF.1.1 The TSF shall enforce the **Row and Column Access Control Policy** to objects based on the following:

a) **Subjects:**

- **User identity**
- **The primary authorization ID of the user**
- **The user role(s) (administration authorities) of the user.**

b) **Objects:**

- **Access control rules for rows associated with a table (row permissions)**
- **Transformation rule for a column associated with a table column (column mask)**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) **When a table has row access control activated and has one or more row permissions associated, then access to a table row is allowed if the row meets the WHERE search condition defined in at least one of the row permissions.**

b) **When a table has column access control activated and the column has a column mask associated, then access to a column value is allowed after applying the CASE expression defined in the table column.**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

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

.

Application note 1: DB2 implements row level access control through the use of row permissions which consists of one or more WHERE clauses that are ORed and appended to any table operation (e.g. select, insert, delete). Similarly, DB2 implements column level access control through the use of column masks, which consist of a CASE clause that is applied on the associated table column and determine the returned value of the table column based on the matched condition.

Application note 2: Row and column access control cannot be used in tables with Mandatory Access Control in Labeled Security Mode (i.e. security label).

6.1.2.5 Complete information flow control ***in DB2*** (FDP_IFC.2(LS-DB2)) (Labeled Security Mode only)

FDP_IFC.2.1 The TSF shall enforce the ***Mandatory Access Control policy*** ~~Multilevel Confidentiality Information Flow Control Policy~~ on

a) Subjects: **DB2 processes acting on behalf of users**;

b) Objects: **rows in tables of DB2 databases**

and all operations that cause that information to flow among them.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow among untrusted subjects and named objects in the TOE are covered by the ***Mandatory Access Control policy***.~~Multilevel Confidentiality Information Flow Control Policy.~~

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:

a) **Database user identifier and~~/or~~ group memberships;**

b) **assigned user roles (DB2 administration authorities); and**

c) **authentication data;**

d) **the sensitivity label; (in Labeled Security Mode)**

g) **In a trusted connection, the database role and/or the sensitivity label (in Labeled Security Mode) defined by the trusted context for the specific user identity.**

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(DB2).

Application note 2: With the exception of attributes assigned by a trusted connection, user attributes are stored in RACF profiles. This Security Target enumerates all user attributes for completeness.

6.1.3.2 User authentication before any action *in DB2* (FIA_UAU.2(DB2))

FIA_UAU.2.1 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 User identification before any action *in DB2* (FIA_UID.2(DB2))

FIA_UID.2.1 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 (administrative authorities).**

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 attributes ***in DB2*** (FMT_MSA.1(DB2))

FMT_MSA.1.1 The TSF shall enforce the **Discretionary Access Control policy** to restrict the ability to **modify, delete** the security attributes **database role** to **authorized administrators**.

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

FMT_MSA.1.1 The TSF shall enforce the **Mandatory Access Control policy** to restrict the ability to **modify** the **label-related object** security attributes **security label of 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.

6.1.4.3 Static attribute initialization ***<u>in DB2</u>*** (FMT_MSA.3(DB2))

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

FMT_MSA.3.2 The TSF shall allow the **authorized administrators** to specify alternative initial values to override the default values when an object or information is created.

6.1.4.4 Static attribute initialization ***<u>for rows in DB2 tables and MAC</u>*** (FMT_MSA.3(LS-DB2)) (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 SFP.

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.

6.1.4.5 Management of TSF data: audit events (FMT_MTD.1(AE-DB2))

FMT_MTD.1.1 The TSF shall restrict the ability to **query, modify** the **set of audited events** to

a) **users with the SECADM user role**

b) **for events related to a profile: the profile owner.**

6.1.4.6 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;

c) creation, modification and deletion of row permissions;

d) activation and deactivation of row access control;

e) creation, modification and deletion of column masks;

f) activation and deactivation of column access control;

g) creation, modification and deletion of audit policies;

h) configuration of audit level on tables.

6.1.4.7 Security roles ***<u>in DB2</u>*** (FMT_SMR.1(DB2))

FMT_SMR.1.1 The TSF shall maintain the ***<u>user</u>*** roles:

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

b) **DB2 System Administrator (SYSADM)**

c) **DB2 System Controller (SYSCTRL)**

d) **DB2 System Operator (SYSOPR)**

e) **DB2 Security administration (SECADM)**

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

g) **DB2 Data Access (DATAACCESS)**

h) **DB2 Access Control (ACCESSCTRL)**

i) **DB2 Installation System Administrator (Install SYSADM)**

j) **DB2 Installation System Operator (Install SYSOPR)**

k) **DB2 Database Administrator (DBADM)**

l) **DB2 Database Controller (DBCTRL)**

m) **DB2 Database Maintainer (DBMAINT)**

n) **DB2 SQL Administrator (SQLADM)**

o) **DB2 Package Administrator (PACKADM)**

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 TSF (FPT)

6.1.5.1 Inter-TSF basic TSF data consistency ***in DB2***: labeled security (FPT_TDC.1(LS-DB2)) (Labeled Security Mode only)

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret label security-related security attributes, **no other TSF data** when shared between the TSF and another trusted IT product.

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

6.2 Security Functional Requirements Rationale

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

6.2.1 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 [OSPP]. 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. 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.

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 in FAU_SEL.1; FAU_SEL.1(DB2) includes additional set of attributes based on the concept of audit policy and the possibility of setting the type of audit at database table level. 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(AS), FMT_MTD.1(AT) and FMT_MTD.1(AF) for the audit storage, and FMT_MTD.1(AE) and FMT_MTD.1(AE-DB2) for the audited events.

Discretionary access control

FDP_ACC.1(PSO) and FDP_ACC.1(TSO) require the existence of a Persistent Storage Object and a Transient Storage Object 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(PSO-MVS), FDP_ACF.1(TSO-MVS), FDP_ACF.1(PSO-UNIX), FDP_ACF.1(TSO-UNIX), FDP_ACF.1(PSO-LDAP) and FDP_ACF.1(TSO-LDAP) in iterations for MVS, UNIX, and LDAP objects. FDP_ACC.2(DB2) defines the discretionary access control policy for DB2 objects and FDP_ACF.1(DB2) defines the rules for access to those objects. Similarly, FDP_ACC.1(RCAC) defines the access control policy for rows and columns in DB2 tables and FDP_ACF.1(RCAC) defines the rules for access to those objects, only for SQL operations (SELECT, UPDATE, INSERT, DELETE). 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(*) and FMT_MSA.1(DB2). When initialized, object attributes are initialized to restrictive values (FMT_MSA.3(DB2) and FMT_MSA.3(LS-DB2), 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(LS), FIA_USB.2 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.2 and FDP_IFC.2(LS-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(LS) 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.1(LS) and FMT_MSA.1(LS-DB2). When new objects are created, proper attribute initialization is ensured by FMT_MSA.3(PSO), FMT_MSA.3(TSO) and FMT_MSA.3(NI) for z/OS objects and FMT_MSA.3(DB2) and FMT_MSA.3(LS-DB2) for DB2 objects.

Import and export of labeled and unlabeled data (FDP_ETC.1, FDP_ETC.2(LS), FDP_ITC.1(LS), FDP_ITC.2 and FDP_ITC.2(LS)) can be provided over a trusted channel . FPT_TDC.1(LS) and FPT_TDC.1(LS-DB2) 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_UAU.2(DB2), FIA_UID.1 and FIA_UID.2(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(*) and FMT_REV.1(USR).

Object reuse

Object reuse (as required by FDP_RIP.2 andFDP_RIP.3) 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(*). 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(IAU) and FMT_REV.1(USR). Because passwords are used for authentication, the management of authentication data is also required in FMT_MTD.1(IAU-AUTH).

Management of the audit system is covered by the requirements for the management of the audit trail (FMT_MTD.1(AS), FMT_MTD.1(AT) and FMT_MTD.1(AF)) and the management of the audit events (FMT_MTD.1(AE) and FMT_MTD.1(AE-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.1(DB2)).

In addition the TOE supports several roles, which is expressed by FMT_SMR.1(DB2).

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

TSF protection

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(*), FCS_CKM.4(*), FCS_COP.1(*) and FCS_RNG.1. Cryptographic services are fully provided by z/OS.

The protocol provides the ability to establish an Inter-TSF trusted channel, as required by FTP_ITC.1.

6.2.2 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 [OSPP] security objectives
FAU_GEN.1(DB2)	O.AUDITING
FAU_GEN.2	O.AUDITING
FAU_SEL.1(DB2)	O.AUDITING
FDP_ACC.2(DB2)	O.DISCRETIONARY.ACCESS
FDP_ACF.1(DB2)	O.DISCRETIONARY.ACCESS
FDP_ACC.1(RCAC)	O.DISCRETIONARY.ACCESS
FDP_ACF.1(RCAC)	O.DISCRETIONARY.ACCESS
FDP_ETC.1	O.LS.CONFIDENTIALITY
FDP_ETC.2(LS)	O.LS.CONFIDENTIALITY
FDP_IFC.2(LS-DB2)	O.LS.CONFIDENTIALITY
FDP_IFF.2(LS)	O.LS.CONFIDENTIALITY
FDP_ITC.1(LS)	O.LS.CONFIDENTIALITY, O.LS.LABEL
FDP_ITC.2	O.DISCRETIONARY.ACCESS, O.SUBJECT.COM
FDP_ITC.2(LS)	O.LS.CONFIDENTIALITY, O.LS.LABEL
FDP_RIP.2	O.AUDITING, O.DISCRETIONARY.ACCESS, O.I&A
FDP_RIP.3	O.AUDITING, O.DISCRETIONARY.ACCESS, O.I&A
FIA_ATD.1(DB2)	O.LS.LABEL
FIA_UAU.2(DB2)	O.I&A
FIA_UID.2(DB2)	O.I&A
FIA_USB.1(DB2)	O.LS.LABEL
FMT_MSA.1(DB2)	O.MANAGE
FMT_MSA.1(LS-DB2)	O.LS.LABEL, O.MANAGE
FMT_MSA.3(DB2)	O.MANAGE
FMT_MSA.3(LS-DB2)	O.LS.LABEL, O.MANAGE
FMT_MTD.1(AE-DB2)	O.MANAGE
FMT_SMF.1(DB2)	O.MANAGE
FMT_SMR.1(DB2)	O.MANAGE
FPT_TDC.1(LS-DB2)	O.LS.CONFIDENTIALITY, O.LS.LABEL

Table 11 - Mapping between SFRs and Security Objectives

6.2.3 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements defined in this ST are suitable to meet and achieve the security objectives. Notice that the security objectives defined in this ST have been defined in [ZOSST], therefore section 7.2.2 of [ZOSST] shall be used in conjunction with this section for completeness.

Security Objectives	Rationale
O.AUDITING	The events to be audited in DB2 are defined in FAU_GEN.1(DB2) and are associated with the identity of the user that caused the event (FAU_GEN.2). The authorized user in must have the capability to specify which

Security Objectives	Rationale
	audit records are generated (FAU_SEL.1(DB2)). The protection of reused resources ensures that no data leaks from other protected sources (FDP_RIP.2, FDP_RIP.3).
O.DISCRETIONARY.ACCESS	The TSF must control access to resources based on the identity of users that are allowed to specify which resources they want to access for storing their data. The access control policy must have a defined scope of control (FDP_ACC.2(DB2) and FDP_ACC.1(RCAC)). The rules for the access control policy are defined (FDP_ACF.1(DB2) and FDP_ACF.1(RCAC)). When import of user data is allowed, the TOE must ensure that user data security attributes required by the access control policy are correctly interpreted (FDP_ITC.2, FPT_TDC.1).The protection of reused resources ensures that no data leaks from other protected sources (FDP_RIP.2, FDP_RIP.3).
O.NETWORK.FLOW	Fully covered by [ZOSST].
O.SUBJECT.COM	Fully covered by [ZOSST].
O.CRYPTO.BASIC	Fully covered by [ZOSST].
O.CRYPTO.NET	Fully covered by [ZOSST].
O.I&A	The TSF must ensure that only authorized users gain access to the TOE and its resources. Users authorized to access the TOE must use an identification and authentication process (FIA_UID.2(DB2), FIA_UAU.2(DB2)). Proper authorization for subjects acting on behalf of users is also ensured (FIA_USB.1(DB2)). The protection of reused resources ensures that no data leaks from other protected sources (FDP_RIP.2, FDP_RIP.3).
O.MANAGE	The TOE provides management interfaces globally defined in FMT_SMF.1(DB2) for the access control policies (FMT_MSA.1(DB2), FMT_MSA.1(LS-DB2), FMT_MSA.3(DB2), FMT_MSA.3(LS-DB2)); The rights management for the different management aspects is defined with FMT_SMR.1(DB2).
O.TRUSTED_CHANNEL	Fully covered by [ZOSST]
O.I&A.REMOTE	Fully covered by [ZOSST]
O.I&A.MULTIPLE	Fully covered by [ZOSST]
O.LS.CONFIDENTIALITY	The information flow control policy is defined by specifying the subjects, objects, security attributes and rules in FDP_IFC.2(LS-DB2) and FDP_IFF.2(LS). Supportive to the enforcement of the policy are the automated label assignment when exporting data (FDP_ETC.1, FDP_ETC.2(LS)) and during the import of data (FDP_ITC.1(LS), FDP_ITC.2(LS)). For assigning labels to imported data, the label information transmitted with the data must be interpretable by the TOE (FPT_TDC.1(LS-DB2)).
O.LS.PRINT	Fully covered by [ZOSST].
O.LS.LABEL	The assignment of labels to users is performed during user-subject binding (FIA_USB.1(DB2)) with security attributes maintained by the TOE (FIA_ATD.1(DB2)). Object labels are assigned to objects when importing them into the TOE (FDP_ITC.1(LS), FDP_ITC.2(LS), FPT_TDC.1(LS-DB2)). The management of labels is allowed for the

Security Objectives	Rationale
	TOE with (FMT_MSA.1(LS-DB2), FMT_MSA.3(LS-DB2)). The label information transmitted with the data must be interpretable by the TOE (FPT_TDC.1(LS-DB2)).

Table 12 - Security objectives for the TOE rationale

6.2.4 Security requirements dependency analysis

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

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

Security Functional Requirement	Dependencies	Resolution	
		DB2	z/OS
FAU_GEN.1(DB2)	FPT_STM.1		FPT_STM.1
FAU_SEL.1(DB2)	FAU_GEN.1	FAU_GEN.1(DB2)	FAU_GEN.1
	FMT_MTD.1	FMT_MTD.1(AE-DB2)	FMT_MTD.1(AE), FMT_MTD.1(AS), FMT_MTD.1(AT), FMT_MTD.1(AF)
FDP_ACC.2(DB2)	FDP_ACF.1	FDP_ACF.1(DB2)	
FDP_ACF.1(DB2)	FDP_ACC.1	FDP_ACC.2(DB2)	
	FMT_MSA.3	FMT_MSA.3(DB2), FMT_MSA.3(LS-DB2)	FMT_MSA.3(PSO), FMT_MSA.3(TSO), FMT_MSA.3(NI), FMT_MSA.3(LS)
FDP_ETC.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.2(DB2), FDP_IFC.2(LS-DB2)	
FDP_ETC.2(LS)	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.2(DB2), FDP_IFC.2(LS-DB2)	
FDP_ACC.1(RCAC)	FDP_ACF.1	FDP_ACF.1(RCAC)	

FDP_ACF.1(RCAC)	FDP_ACC.1
	FMT_MSA.3
		FDP_ACC.1(RCAC)
		FMT_MSA.3(DB2)	

FDP_IFC.2(LS-DB2)	FDP_IFF.1		FDP_IFF.2(LS)
FDP_IFF.2(LS)	FDP_IFC.1	FDP_IFC.2(LS-DB2)	FDP_IFC.2(LS)
	FMT_MSA.3	FMT_MSA.3(DB2), FMT_MSA.3(LS-DB2)	FMT_MSA.3(PSO), FMT_MSA.3(TSO), FMT_MSA.3(NI) , FMT_MSA.3(LS)
FDP_ITC.1(LS)	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.2(DB2), FDP_IFC.2(LS-DB2)	
	FMT_MSA.3	FMT_MSA.3(DB2), FMT_MSA.3(LS-DB2)	FMT_MSA.3(PSO), FMT_MSA.3(TSO), FMT_MSA.3(NI) , FMT_MSA.3(LS)

FDP_ITC.2(LS)	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.2(DB2), FDP_IFC.2(LS-DB2)	
FDP_RIP.2	None		
FDP_RIP.3	None		
FIA_ATD.1(DB2)	None		
FIA_UAU.2(DB2)	FIA_UID.1	FIA_UID.2(DB2)	
FIA_UID.2(DB2)	None		
FIA_USB.1(DB2)	FIA_ATD.1	FIA_ATD.1(DB2)	
FMT_MSA.1(DB2)	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.2(DB2)	
	FMT_SMF.1	FMT_SMF.1(DB2)	
	FMT_SMR.1	FMT_SMR.1(DB2)	
FMT_MSA.1(LS-DB2)	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.2(DB2)	
	FMT_SMF.1	FMT_SMF.1(DB2)	
	FMT_SMR.1	FMT_SMR.1(DB2)	
FMT_MSA.3(DB2)	FMT_MSA.1	FMT_MSA.1(DB2)	
	FMT_SMR.1	FMT_SMR.1(DB2)	
FMT_MSA.3(LS-DB2)	FMT_MSA.1	FMT_MSA.1(LS-DB2)	
	FMT_SMR.1	FMT_SMR.1(DB2)	
FMT_MTD.1(AE-DB2)	FMT_SMF.1	FMT_SMF.1(DB2)	
	FMT_SMR.1	FMT_SMR.1(DB2)	
FMT_SMF.1(DB2)	None		
FMT_SMR.1(DB2)	FIA_UID.1	FIA_UID.2(DB2)	
FPT_TDC.1(LS-DB2)	None		

Table 13 - SFR Dependencies

6.3 TOE security assurance requirements

The security assurance requirements for the TOE correspond to Evaluation Assurance Level 4, augmented by ALC_FLR.3, as specified in [CC] part 3. This conformance claims are aligned with the conformance claims specified in the [ZOSST].
The [ZOSST] includes a refinement on ASE_CCL.1(CCR) that is included in the OSPP base. This operation does not put an additional requirement on the product but requires the evaluator to check that all ST author notes from the PP have been dealt with in the security target. Please refer to [ZOSST] for more information.

6.4 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 [OSPP].

6.5 TOE Summary Specifications Rationale

6.5.1 Security functions justification

The following table maps the security functional requirements to the security functions as defined in the TOE summary specification to show that all security functional requirements are addressed by the security functions. Notice that only the SFRs enforced by DB2 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 8.1.6 of [ZOSST].
FAU_GEN.2	Section 7.6.1 explains the context information DB2 and z/OS generate in the audit records. Further explanation of the auditing functionality can be found in section 8.1.6 of [ZOSST].
FAU_SEL.1(DB2)	Section 7.6.1 explains how system and database administrators can configure the events that are audited through the use of audit policies and specifying audit at table level. Additionally, section 8.1.6.5 in [ZOSST] explains how the auditor role can configure the events that are audited, and that the owner of a profile can define which events related to the profile are audited.
FDP_ACC.2(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_ACC.1(RCAC)	Row and column access control policy for DB2 is explained in section 7.3.6.
FDP_ACF.1(RCAC)	Row and column access control policy for DB2 is explained in section 7.3.6.
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 8.1.3.4 of [ZOSST].
FDP_ETC.2(LS)	Export of labeled data is explained in Section 7.3.3.1. Further explanation can be found in section 8.1.3.2, “Mandatory Access Control (Labeled Security Mode only)” of [ZOSST].
FDP_IFC.2(LS-DB2)	The mandatory access control policy for DB2 is explained in Section 7.3.3.1. Further explanation can be found in section 8.1.3.2, “Mandatory Access Control (Labeled Security Mode only)” of [ZOSST].
FDP_IFF.2(LS)	The mandatory access control policy for DB2 is explained in Section 7.3.3.1. Further explanation can be found in section 8.1.3.2, “Mandatory Access Control (Labeled Security Mode only)” of [ZOSST].
FDP_ITC.1(LS)	Import of unlabeled user data is explained in Section 7.3.3.1. Further explanation can be found in section 8.1.3.4 of [ZOSST]).
FDP_ITC.2	Import of unlabeled user data is explained in Section 7.3.3.1. Further explanation can be found in section 8.1.3.4 of [ZOSST]).
FDP_ITC.2(LS)	Import of labeled user data is explained in Section 7.3.3.1. Further explanation can be found in section 8.1.3.4 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 8.1.7 of [ZOSST].

SFR	Security Functions
FDP_RIP.3	Object reuse for DB2 objects is described in section 7.7.2; object reuse for z/OS objects is described in Section 8.1.7 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 8.1.2 of [ZOSST].
FIA_UAU.2(DB2)	User authentication to DB2 is explained in sections 7.2.1 and 7.2.2. Further explanation can be found in section 8.1.2 in [ZOSST].
FIA_UID.2(DB2)	User identification to DB2 is explained in sections 7.2.1 and 7.2.2. Further explanation can be found in section 8.1.2 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 8.1.2 in [ZOSST].
FMT_MSA.1(DB2)	Management of object security attributes is explained in section 7.5.2 of this ST, and in section 8.1.5 (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. RACF configuration is also described.
FMT_MSA.1(LS-DB2)	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.3(DB2)	DB2 security management is explained in section 7.5.2. Default values for the access control are defined in the UACC attribute in the resource profiles as explained in section 8.1.5.2 of [ZOSST] in the description of the resource profiles.
FMT_MSA.3(LS-DB2)	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(AE-DB2)	Audit event management is explained in sections 7.5.2 and 7.6.1 of this ST and section 8.1.6.5 of [ZOSST].
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 8.1.5.1, “User roles and attributes” of [ZOSST].
FPT_TDC.1(LS-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.

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
- Through an external entity that establishes a trusted connection, authorized by the association with a trusted context (see section 7.2.3)

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).

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).

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 RRSAF), the RACF user id (for RRSAF) or the TSO logon ID (for TSO).
- The job or started task name

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

- The system authorization ID which is determined either by a set of rules included in the SYSIBM catalog tables[1] (for z/OS requesters), derived from the authentication token (for z/OS servers[2]), or otherwise derived from the user id provided by the external entity (e.g. a middleware server).

[1] For more information, see “Establishing remote trusted connections by DB2 for z/OS requesters” in the DB2 11 for z/OS Managing Security.

[2] For more information, see “Establishing remote trusted connections to DB2 for z/OS servers” in the DB2 11 for z/OS Managing Security.

- 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 to model DB2 administrative authorities, DB2 privileges and DB2 objects, 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 through 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.
- 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 statement[3]. 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).

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).

In order to export a table that has multilevel security with row-level granularity, the user must have an accessible valid security label. Each row is exported only if the security label dominates the data security label. 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.

Likewise, to import of data with multilevel security and row-level granularity, the user must have an accessible valid security label. The user must have the write-down privilege to specify values for the security label; otherwise, the TOE assigns the user security label for the security label column for the rows that are being imported (AC.3-DB2-7).

[3] 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.

The column used as the security label cannot be dropped from the table.

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, groups and administrative authorities assigned to, database 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
  - Row permission
  - Column mask
  - Global variable
- 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 database role. In trusted connections, role ownership in DB2 objects and the role assigned to the process based on the trusted context definition are taking into account in the Discretionary Access Control policy. In non-trusted connections, only authorization ID ownership is used.

Note that rows are not objects that are subject to discretionary access control through RACF. Row and column access control provides additional discretionary access control on a finer granularity; see section 7.3.6.

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

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

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

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

RACF has the following classes defined for DB2 objects:

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

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

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

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

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

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

DB2 object	Object name qualifiers
Buffer pool	*bufferpool-name*
Collection	*collection-ID*

DB2 object	Object name qualifiers
Database	*database-name*
Java archive (JAR)	*schema-name.JAR-name*
Package	*collection-ID.package-ID* *collection-ID* *owner*
Plan	*plan-name* *owner*
Role	not applicable
Schema	*schema-name* *schema-name.function-name* *schema-name.procedure-name* *schema-name.type-name*
Sequence	*schema-name.sequence-name*
Storage group	*storage-groupname*
Stored procedure	*schema-name.procedure-name*
System	*owner*
Table, index	*table-qualifier.table-name* *table-qualifier.table-name.column-name*
Tablespace	*database-name.table-space-name*
Trusted context	not applicable
User-defined distinct type	*schema-name.type-name*
User-defined function	*schema-name.function-name*
View	*view-qualifier.view-name* *table-qualifier.table-name.view-qualifier.view-name* *table-qualifier.table-name.column-name.view-qualifier.view-name*
Global variable	*schema- name.variable-name*

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

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

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

In this case the following algorithm is used to evaluate the access right a user has to a DB2 privilege or DB2 administration authority to a DB2 object:

1. If the user has a specific DB2 administration authority, granted by the implicit rights of an administration authority, access is granted (AC.4-DB2-1)
2. If the user is the owner of the DB2 object and the requested DB2 administration authority is granted to the owner of the object, access is granted (AC.4-DB2-2a)
3. In a trusted connection, if there is a database role assigned, the database role is the owner of the DB2 object and the requested DB2 administrative authority is granted to the owner of the object, access is granted (AC.4-DB2-2b)
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 7.3.4.3 to 7.3.4.21), access is granted (AC.4-DB2-4).
6. If the user (as defined by the primary authorization ID) has sufficient the TRUSTED or PRIVILEGED attribute, access is granted (AC.4-DB2-4b).
7. 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).
8. 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 7.3.4.3 to 7.3.4.21), access is granted (AC.4-DB2-6)
9. 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).
10. 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 7.3.4.3 to 7.3.4.21), access is granted (AC.4-DB2-8)
11. 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).

12. If a user ID of * is found on the standard access list of the RACF profile protecting any type of DB2 privilege that allows access (according to the description in sections 7.3.4.3 to 7.3.4.21) provides sufficient access (see Note) and the current user is defined to RACF without the RESTRICTED attribute, access is granted (AC.4-DB2-10)
13. 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).
14. If the universal access authority (UACC) for the RACF profile protecting any type of DB2 privilege that allows access (according to the description in sections 7.3.4.3 to 7.3.4.21) provides sufficient access (see Note) and the current user is defined to RACF without the RESTRICTED attribute, access is granted (AC.4-DB2-12).
15. 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).
16. 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).
17. 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).
18. 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).
19. 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 (a database role is only valid in trusted connections).

7.3.4.3 DB2 administrative authorities

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

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

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

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

The following subchapters specify for each DB2 object protected by RACF, the DB2 authorities defined for the object and the RACF profile protecting the DB2 privilege for the DB2 object that the user requires sufficient access to.

See the Note at the end of Section ‘Access evaluation algorithm for DB2 objects’ on page 62 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 DB2 objects for owner ACEE authorization

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

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

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

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

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

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

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

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

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

7.3.4.5 Buffer pool privileges

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

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

7.3.4.6 Collection privileges

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

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

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

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

- The user has sufficient access to the resource *DB2-subsystem.collection-ID*.CREATEIN in the MDSNCL or GDSNCL class (AC.4-DB2-23)
- The user has sufficient access to the resource *DB2-subsystem.collection-ID*.PACKADM in the DSNADM class (AC.4-DB2-24)
- The user has sufficient access to the resource *DB2-subsystem.* SYSDBADM in the DSNADM class (AC.4-DB2-24a)
- The user has sufficient access to *DB2-subsystem*.SYSCTRL in the DSNADM class (AC.4-DB2-25)
- The user has sufficient access to *DB2-subsystem*.SYSADM in the DSNADM class (AC.4-DB2-26)

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

7.3.4.8 Java archive privileges

Java archives are not part of the evaluated configuration.

7.3.4.9 Package privileges

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

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

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

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

SDP: only for system defined packages

7.3.4.10 Plan privileges

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

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

7.3.4.11 Role privileges

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

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

SSN: Only when SEPARATE_SECURITY parameter = ”No”

7.3.4.12 Schema privileges

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

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

7.3.4.13 Sequence privileges

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

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

7.3.4.14 Storage group privileges

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

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

7.3.4.15 Stored procedure privileges

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

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

SDP: only for System Defined Packages

7.3.4.16 DB2 system privileges

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

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

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

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

7.3.4.17 Table privileges

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

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

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

T: only tables (not views)

SCT: only for system catalog tables

SSN: only when SEPARATE_SECURITY parameter = "No"

APE: SYSIBM.SYSAUDITPOLICIES table excluded

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

7.3.4.18 Tablespace privileges

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

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

7.3.4.19 Trusted context privileges

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

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

SSN: Only when SEPARATE_SECURITY parameter = ”No”

7.3.4.20 View privileges

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

Specific view privilege	Owner of view	Privilege in view class	DBADM	SYSCTRL	SYSADM	SYSDBADM	SQLADM	DATAACCESS	ACCESSCTRL	SECADM
ALTER	X			X	X	X				
COMMENT ON	X			X	X	X				
DELETE (for updatable views)	X	X	X		X	SCT APE	SCT APE	APE	SCT APE	SCT
DELETE (for read-only views)		X			X			X		
DROP	X			X	X	X				
INSERT (for updatable views)	X	X	X		X	SCT APE	SCT APE	APE	SCT APE	SCT
INSERT (for read-only views)		X			X			X		
INSTEAD OF TRIGGER	X			X	X	X				
REGENERATE VIEW	X			X	X	X				
SELECT		X			X			X		
UPDATE (for updatable views)	X	X	X		X	SCT APE	SCT APE	APE	SCT APE	SCT

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

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

SCT: only System Catalog Tables

APE: SYSIBM.SYSAUDITPOLICIES table excluded

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

7.3.4.21 Global variable privileges

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

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

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

7.3.4.22 Row permissions

There are no explicit privileges for this DB2 object: the user must have the SECADM administration authority to create or alter permissions (AC.4-DB2-44).

7.3.4.23 Column masks

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

7.3.4.24 Specifics of discretionary access control when in Labeled Security Mode

The tables in sections 7.3.4.3 to 7.3.4.20 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.

7.3.6 Row and Column access control

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

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

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

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

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

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

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

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

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
4. Management of row and column access control

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 SQLADM, SYSDBADM, SECADM, SYSOPR, SYSCTRL or SYSADM authority or users with the TRACE privilege (SM.3-DB2-4). Setting or modifying the audit attribute of a table requires either SYSDBADM, SYSADM or SYSCTRL authority, DBADM authority for the database the table is part of, ownership of the table or ALTER privilege on the table (SM.3-DB2-5).

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

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

Column masks are DB2 objects managed using the CREATE MASK, ALTER MASK and DROP SQL commands (SM.3-DB2-11); column access control can also be activated or deactivated with the ACTIVATE, DEACTIVATE COLUMN ACCESS CONTROL clause of the ALTER TABLE statement (SM.3-DB2-12). Control access to users on these objects and their management operations is performed by RACF as the rest of the DB2 objects.

7.5.3 DB2 user attributes and user roles and database roles

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

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

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

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

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

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

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

User roles are defined by dedicated profiles in the DSNADM class (SM.3-DB2-6). A user gets a user role assigned when he is assigned sufficient access [4] to the profile associated with the user role (SM.3-DB2-7). This can be done by any user that is allowed to assign permission to those profiles according to the rules implemented in RACF. The privileges associated with each role are defined in the description of the discretionary access rights in this ST.

7.5.4 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

[4] 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.

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

Audit class	Audit events that are traced
1	Access attempts that DB2 denies because of inadequate authorization (AU.3-DB2-5). This class is the default.
2	Explicit GRANT and REVOKE statements and their results. This class does not trace implicit grants and revokes. Note that GRANT and REVOKE have no effect in the evaluated configuration and therefore those events are not security relevant. **Note that this has no meaning in the evaluated configuration.**
3	Traces CREATE, ALTER, and DROP operations against an audited tables or a table that is enabled with multilevel security with row-level granularity. For example, it traces the deletion of a table as the result of a DROP TABLESPACE or DROP DATABASE; it also traces the updates to a table created with the AUDIT CHANGES or AUDIT ALL clause (AU.3-DB2-6).
4	Changes to audited tables. Only the first attempt to change a table, within a unit of recovery, is recorded. (If the agent or the transaction issues more than one COMMIT statement, the number of audit records increases accordingly.) The changed data is not recorded, only the attempt to make a change is recorded. If the change is not successful and is rolled back, the audit record remains; it is not deleted. This class includes access by the LOAD utility. Accesses to a dependent table that are caused by attempted deletions from a parent table are also audited. The audit record is written even if the delete rule is RESTRICT, which prevents the deletion from the parent table. The audit record is also written when the rule is CASCADE or SET NULL, which can result in deletions that cascade to the dependent table (AU.3-DB2-7).
5	All read accesses to tables that are identified with the AUDIT ALL clause. As in class 4, only the first access within a DB2 unit of recovery is recorded. References to a parent table are also audited (AU.3-DB2-8).
6	The bind of static and dynamic SQL statements of the following types: • INSERT, UPDATE, DELETE, CREATE VIEW, and LOCK TABLE statements for audited tables. Except for the values of host variables, the audit record contains the entire SQL statement (AU.3-DB2-9). • SELECT statements on tables that are identified with the AUDIT ALL clause. Except for the values of host variables, the audit record contains the entire SQL statement (with record type IFCID 0350 included) (AU.3-DB2-10).
7	Assignment or change of an authorization ID because of the following reasons (AU.3-DB2-11): • Changes through a default or user-written exit routine (not relevant for the evaluated configuration). • Changes through a SET CURRENT SQLID statement • An outbound or inbound authorization ID translation (inbound translation is not relevant for the evaluated configuration) • An ID that is being mapped to a RACF ID from a Kerberos security ticket (not relevant for the evaluated configuration)
8	The start of a utility job, and the end of each phase of the utility.
9	Various types of records that are written to IFCID 0146 by the IFI WRITE function.

Audit class	Audit events that are traced
10	CREATE and ALTER TRUSTED CONTEXT statements, establish trusted connection information and switch user information
11	Audit the use of any DB2 administrative authority and the successful execution of any authorization ID.

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).

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

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

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

Audit Category	Description
CHECKING	Generates IFCID 140 trace records for denied access attempts due to inadequate DB2 authorization and IFCID 83 trace records for RACF authentication failures
VALIDATE	Generates IFCID 55, 83, 87, 169, and 319 trace records for new or changed assignments of authorization IDs and IFCID 269 trace records for the establishment of trusted connections or the switch of users in existing trusted connections.
OBJMAINT	Generates IFCID 142 trace records when tables are altered or dropped.
EXECUTE	Generates IFCID 143 and 144 trace records for SQL statement and generates IFCID 145 records to trace bind time information about SQL statements that involve audited objects.
CONTEXT	Generates IFCID 23, 24, and 25 records.
SECMAINT	Generates IFCID 270 trace records for creating and altering trusted contexts, and IFCID 271 trace records for creating, altering, and dropping row permissions or column masks. Generates also IFCID 141 trace records for granting and revoking privileges or administrative authorities, but this record is not generated in the evaluated

Audit Category	Description
	configuration, as privileges and administrative authorities are maintained through RACF.
SYSADMIN	Generates IFCID 361 trace records when an administrative authority, in the order of installation SYSADM, installation SYSOPR, SYSOPR, SYSCTRL, or SYSADM, satisfies the required privilege for performing an operation. This category is not allowed in the evaluated configuration as it is not supported by the RACF exit.
DBADMIN	Generates IFCID 361 trace records when an administrative authority, in the order of DBMAINT, DBCTRL, DBADM, PACKADM, SQLADM, system DBADM, DATAACCESS, ACCESSCTRL, or SECADM, satisfies the required privilege for performing an operation. This category is not allowed in the evaluated configuration as it is not supported by the RACF exit.

Table 17 - Audit Categories

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

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

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

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

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
CC	Common Criteria
DAC	Discretionary Access Control
CPACF	Central Processor Assist for Cryptographic Functions
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
LSPP	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
RVA	RAMAC Virtual Array
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

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 [OSPP]; 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.

Audit Policy

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

Buffer Pool

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

Collection

A collection of packages

Column

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

Column mask

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

Database

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

Database Role

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

DB2 object

The DB2 objects are defined in section 7.3.4.1.

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 an aggregate function or a scalar function. A user-defined function can be a column, scalar, or table function.

Index

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

Java Archive

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

Package

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

Plan

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

A list of package names

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

Primary authorization ID

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

Row

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

Row Permission

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

Schema

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

Sequence

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

Storage Group

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

Stored Procedure

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

Subsystem or data sharing group

A distinct instance of DB2.

Table

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

Tablespace

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

Trigger

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

Trusted Context

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

View

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

8.3 References

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

[BSI-ZOS] Common Criteria (CC) Protection Profiles for IT products (Schutzprofile nach Common Criteria (CC) für IT-Produkte)
Location
https://www.bsi.bund.de/SharedDocs/Zertifikate/CC/Betriebssysteme/0788.html

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

[DB2AG] DB2 11 for z/OS Administration Guide
Document Number: TBC

[DB2API] DB2 11 for z/OS Application Programming and SQL Guide
Document Number: TBC

[DB2CCG] DB2 11 for z/OS Common Criteria Guide
Document Number: TBC

[DB2CR] DB2 11 for z/OS Command Reference
Document Number: TBC

[DB2IG] DB2 11 for z/OS Installation Guide
Document Number: TBC

[DB2INT] DB2 11 for z/OS Introduction to DB2 for z/OS
Document Number: TBC

[DB2ACMG] DB2 11 for z/OS RACF Access Control Module Guide
Document Number: TBC

[DB2WN DB2 11 for z/OS What’s New
Document Number: TBC

[DB2SQL] DB2 11 for z/OSSQL Reference
Document Number: TBC

[DB2UGR] DB2 11 for z/OS Utility Guide and Reference
Document Number: TBC

[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

[OSPP] Operating System Protection Profile
Version 2.0, 2010-06-01 (certification ID BSI-CC-PP-0067-2010)

[OSPP-EIA] OSPP Extended Package -- Extended Identification and Authentication
Version 2.0, 2010-05-28 (certification ID BSI-CC-PP-0067-2010)

[OSPP-LS] OSPP Extended Package -- Labeled Security
Version 2.0, 2010-05-28 (certification ID BSI-CC-PP-0067-2010)

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

[ZOSST] Security Target for IBM z/OS Version 1 Release 13
Version 9.02
2012-09-09

End of document