collaborative Protection Profile for Database Management Systems

12 June 2020

Version 1.0

Acknowledgements

This collaborative Protection Profile (cPP) was developed by the Database Management System international Technical Community with representatives from industry, Government agencies, Common Criteria Test Laboratories. The organizations that contributed to the development of this cPP include:

Industry

IBM

Microsoft

Oracle Corp.

Common Criteria Test Laboratories

atsec information security

Intertek EWA-Canada and Intertek Acumen

TÜViT

Teron Labs

Government Agencies

FMV/CSEC - Swedish Certification Body for IT Security

BSI - Bundesamt für Sicherheit in der Informationstechnik

JISEC - Japan IT Security Evaluation and Certification Scheme

Details of how to contact the DBMS iTC are found on the Common Criteria Portal at:

https://www.commoncriteriaportal.org/communities/index.cfm

0. Preface

0.1 Objectives of Document

This document presents the Common Criteria (CC) collaborative Protection Profile (cPP) to express the security functional requirements (SFRs) and security assurance requirements (SARs) for a Database Management System. The Evaluation Activities that specify the actions the evaluator performs to determine if a product satisfies the SFRs captured within this cPP are described in the associated Supporting Document.

0.2 Scope of Document

The scope of the cPP within the development and evaluation process is described in the Common Criteria for Information Technology Security Evaluation [CC1]. In particular, a cPP defines the IT security requirements of a generic type of TOE and specifies the functional and assurance security measures to be offered by that TOE to meet stated requirements [[CC1], Section C.1].

0.3 Intended Readership

The target audiences of this cPP are DBMS developers, CC consumers, system integrators, CC evaluators and CCRA schemes.

Although the cPPs and SDs may contain minor editorial errors, cPPs are recognized as living documents and the iTCs are dedicated to ongoing updates and revisions. Please report any issues to the DBMS iTC. Information on how to contact the DBMS iTC can be found on the Technical Communities information page.

0.4 Related Documents

The following documents are available from the CC Portal at https://www.commoncriteriaportal.org/

Common Criteria

[CC1] Common Criteria for Information Technology Security Evaluation,
Part 1: Introduction and General Model,
CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.
https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2: Security Functional Components,
CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.
https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3: Security Assurance Components,
CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

[CEM] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
CCMB-2017-04-004, Version 3.1 Revision 5, April 2017
https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf

Documents related to this cPP

[SD] Supporting Document Mandatory Technical Document Evaluation Activities for the collaborative Protection Profile for Database Management Systems, Version 1.0, 12 June 2020

Other Documents

[DBMSiTC] DBMS iTC Status
https://www.commoncriteriaportal.org/files/communities/Status.DBMS.pdf

[CCADD] CC and CEM Addenda: Exact Conformance, Selection-Based SFRs, Optional SFRs
CCDB-2017-05-xxx, Version 0.5, May 2017

0.5 Conventions

Except for replacing United Kingdom spelling with American spelling, the notation, formatting, and conventions used in this cPP are consistent with version 3.1 of the CC. Selected presentation choices are discussed here to aid the cPP reader.

The CC allows several operations to be performed on functional requirements; *refinement, selection, assignment*, and *iteration* are defined in clause 8 of Part 1 of the CC [CC1]. Each of these operations is used in this Protection Profile (PP).

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by bold text or in the case of deletions, by **~~crossed out bold text~~**.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted by *italicized text*, selections to be filled in by the Security Target (ST) author

appear in square brackets with an indication that a selection is to be made, [selection:], and are not italicized.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the cPP authors are denoted by showing the value in square brackets, [assignment_value], assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:].

The **iteration** operation is used when a component is repeated with varying operations.

Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration number).

The CC paradigm also allows protection profile authors to create their own requirements. Such requirements are termed “extended requirements” and are permitted if the CC does not offer suitable requirements to meet the author’s needs. Extended requirements must be identified and are required to use the CC class/family/component model in articulating the requirements. In this cPP, extended requirements will be indicated with the “_EXT” following the component name.

Application Notes are provided to help the developer, either to clarify the intent of a requirement, identify implementation choices, or to define “pass-fail” criteria for a requirement. For those components where Application Notes are appropriate, the Application Notes will follow the requirement component. They are numbered and formatted thus:

Application Note 1: *This is an application note.*

0.6 Revision History

Version	Date	Description
0.01	14th February, 2019	Initial Release for iTC review
0.02	8th March, 2019	After iTC workshop review
0.03	16th June, 2019	Updated with the agreed SPD[1] (V1.0) after Public Review
0.04	28th October, 2019	Updates by iTC
0.05	7 February 2020	Acceptance of changes, formatting changes
0.06	28 February 2020	Acceptance of changes
1.0	16 June 2020	Initial Release

[1] Security Problem Definition

Contents

Figures / Tables

1. cPP Introduction

1.1 cPP Reference Identification

cPP Reference: collaborative Protection Profile for Database Management Systems

cPP Version: 1.0

cPP Date: 12 June 2020

1.2 cPP Overview

This is a collaborative Protection Profile (cPP), a PP that meets the requirements for cPPs described in the Common Criteria Recognition Arrangement.

Security Targets (STs) that claim conformance to this cPP shall claim exact conformance as defined in Addenda for Exact conformance the CC, [CCADD]

The product type of the Target of Evaluation (TOE) described in this cPP is a database management system (DBMS). A database is an organized collection of data, generally stored and accessed electronically from a computer system. The database management system (DBMS) is the software that interacts with end users, applications, and the database itself to capture and analyze the data. The DBMS software additionally encompasses the core facilities provided to administer the database. A DBMS may be a single-user system, in which only one user may access the DBMS at a given time, or a multi-user system, in which many users may access the DBMS simultaneously.

The DBMS will have the capability to limit DBMS access to authorized users, enforce Discretionary Access Controls (DAC) on objects under the control of the database management system based on user and optionally, group authorizations, and provide user accountability via audit of users' actions.

This cPP specifies security requirements for a commercial-off-the-shelf (COTS) database management system (DBMS). The TOE type is a database management system.

Security Targets (ST) derived from this cPP describe Targets of Evaluation (TOE) that are Database Management Systems.

1.3 TOE Overview

A TOE compliant with this cPP includes, but is not limited to, a DBMS server and can be evaluated as a software only application layered on an underlying system, i.e., an operating system (OS), hardware, network services, and/or custom software, and is usually embedded as a component of a larger system within an operational environment. This profile establishes the requirements necessary to achieve the security objectives of the Target of Evaluation (TOE) and its environment.

Conformant TOEs provide access control based on user identity and, optionally, group membership, e.g., Discretionary Access Control (DAC), and generation of audit records for security relevant events. Authorized administrators of the TOE are trusted to not misuse the privileges assigned to them.

1.3.1 Database Management Systems overview

A DBMS is comprised of the DBMS server application that performs some or all of the following functions:

a) Controlling TOE users' accesses to user data and TSF data;
b) Indexing data values to their physical locations for quick retrievals based on a value or range of values;
c) Executing pre-written programs (i.e., utilities) to perform common tasks like database backup, recovery, loading, and copying;
d) Supporting mechanisms that enable concurrent database access (e.g., locks);
e) Assisting recovery of user data and DBMS data (e.g., transaction log); and
f) Tracking operations that users perform.

Most commercial DBMS server applications also provide the following functions:

- A data model with which the DBMS data structures and organization can be conceptualized (e.g., hierarchical, object-oriented, relational data models) and DBMS objects defined.
- High-level language(s) or interfaces that allow authorized users to define database constructs; access and modify user or DBMS data; present user or DBMS data; and perform operations on those data.

A DBMS supports two user types:

1. Users who interact with the DBMS to observe and/or modify data objects for which they have authorization to access; and
2. The authorized administrators who implement and manage the various information-related policies of an organization (e.g., access, integrity, consistency, availability) for the databases that they install, configure, manage, and/or own.

A DBMS stores and controls access to two types of data:

1. The first type is the user data that the DBMS maintains and protects. User data may consist of the following:
   a) The user data stored in or as database objects;
   b) The definitions of user databases and database objects, commonly known as DBMS metadata; and
   c) The user-developed queries, functions, or procedures that the DBMS maintains for users.
2. The second type is the DBMS data (e.g., configuration parameters, user security attributes, transaction log, audit instructions, and records) that the DBMS maintains and may use to operate the DBMS.

DBMS specifications identify the detailed requirements for the DBMS server functions given in the above list.

1.3.2 Security Functionality Provided by the TOE

A DBMS evaluated against this PP will provide the following security services.

Security services that must be provided by the TOE:

- Discretionary Access Control (DAC) limits access to objects based on the identity of the subjects or groups to which the subjects and objects belong, and which allows authorized users to specify how the objects that they control are protected.
- Audit Capture for creation of information on all auditable events.
- Authorized administration role to allow authorized administrators to configure the policies for discretionary access control, identification and authentication, and auditing. The TOE must enforce the authorized administration role.
- Limitation of the number of concurrent sessions and restrictions on establishing sessions.

Application Note 1: *Some administrative tasks may be delegated to specific users (which by that delegation become administrators although they can only perform some limited administrative actions). Ensuring that those users cannot extend the administrative rights assigned to them is a security functionality the TOE has to provide.*

1.3.3 TOE definition

The TOE consists of at least one instance of the security functions of the DBMS server application with its associated guidance documentation and the interfaces to the external Information Technology (IT) entities with which the DBMS interacts.

This cPP does not dictate a specific architecture. The ST writer will need to identify and describe the TOE architecture to be evaluated. Architectures are described in Section 1.4.2.

The external IT entities, with which the DBMS may interact, may include the following:

- Client applications that allow users to interface with the DBMS server.
- The host operating system (host OS) on which the TOE has been installed;
- The networking, printing, data-storage, and other devices and services with which the host OS may interact on behalf of the DBMS or the DBMS user; and the other IT products such as application servers, web servers, authentication servers, directory services, and transaction processors with which the DBMS may interact to perform a DBMS function or a security function.

The TOE Security Function (TSF) is limited to the elements required to exercise the evaluated security functionality.

The DBMS must specify the host OS on which it must reside to provide the desired degree of security feature integration as well as the configuration of those OS(es) required to support the DBMS functions. In all cases, the TOE must be installed and administered in accordance with the TOE installation and administration instructions.

1.3.4 Limitations of Security Claims

Conformance with this cPP will not guarantee the following:

- Physical protection mechanisms and the administrative procedures for using them are in place.
- Mechanisms to ensure the complete availability of the data residing on the DBMS are in place. The DBMS can provide simultaneous access to data to make the data available to more than one person at a given time, and it can enforce DBMS resource allocation limits to prevent users from monopolizing a DBMS service/resource. However, it cannot detect or prevent the unavailability that may occur because of a physical or environmental disaster, a storage device failure, or external threats on the underlying operating system. For such threats to availability, the environment must provide the required countermeasures.
- Mechanisms to ensure that users properly secure the data that they retrieve from the DBMS are in place. The security procedures of the organization(s) that use and manage the DBMS must define users' data retrieval, storage, export, and disposition responsibilities.
- Mechanisms to ensure that authorized administrators wisely use DAC. Although the DBMS can support an access control policy by which users and optionally users in defined groups, are granted access only to the data that they need to perform their jobs, it cannot completely ensure that authorized administrators who are able to set access controls will do so prudently.

1.4 TOE Operational Environment

1.4.1 DBMS Architecture and Environmental Components

This cPP does not dictate a specific architecture. A TOE compliant with this cPP may be evaluated and may operate in several architectures, including, but not limited to, one or more of the following:

- A stand-alone system running the DBMS server application; a stand-alone system running the DBMS server and DBMS client(s) and serving one, or more than one, online user at a given time;
- A network of systems communicating with several distributed DBMS servers simultaneously;
- A network of workstations or terminals running DBMS clients and communicating with a DBMS server simultaneously; these devices may be hardwired to the host computer or be connected to it by means of local or wide-area networks; and
- A network of workstations communicating with one or more application servers, which in turn interact with the DBMS on behalf of the workstation users or other subjects (e.g., a DBMS server interacting with a transaction processor that manages user requests).

1.4.2 TOE Administration

This cPP defines one necessary administrator role (authorized administrator) which is established by the developer of the DBMS. This cPP allows the DBMS developer or security target writer to define more user or administrator roles.

If the security target allows it, the administrators of the system may assign privileges to users. When the DBMS is established, the ability to assign privileges and their associated responsibilities must also exist.

Authorized administrators of the TOE will have capabilities that are commensurate with their assigned administrative privileges. The very ability to establish and assign privileges will itself be a privileged function.

2. Conformance Claims

2.1 Conformance with CC

This cPP conforms to the requirements of Common Criteria v3.1, Revision 5 as defined by the references [CC1], [CC2] and [CC3], The methodology applied for the PP evaluation is defined in [CEM].

This cPP also applies the CC and CEM Addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs: V0.5 dated May 2017 noting that it is labelled as “for trial use”.

This cPP satisfies the following Assurance Families: APE_CCL.1, APE_ECD.1, APE_INT.1, APE_OBJ.2, APE_REQ.2 and APE_SPD.1.

2.2 Conformance with CC parts 2 and 3

DBMS PP is CC version 3.1 revision 5 Part 2 extended and Part 3 conformant.

2.3 Conformance with Packages

The DBMS cPP does not claim conformance to any functional packages.

The DBMS cPP claims conformance to the EAL2 assurance package augmented by ALC_FLR.3 Systematic flaw remediation.

2.4 Conformance with other Protection Profiles

The DBMS cPP does not claim conformance to any other Protection Profile.

2.5 Conformance Statement

DBMS cPP requires exact conformance by an ST.

Exact Conformance is a subset of Strict Conformance as defined by [CC1]. Exact Conformance is defined as the ST containing all of the SFRs in section 5 (these are mandatory SFRs) of this cPP, and potentially SFRs from Appendix A (these are optional SFRs). While iteration is allowed, no additional requirements from [CC2], [CC3], or definitions of extended components not already included in this cPP) are allowed to be included in the ST. Further, no SFRs in section 5 of this cPP are allowed to be omitted.

2.6 PP-Configuration

The collaborative Protection Profile for Database Management Systems (DBMS PP) is structured as a base Protection Profile, able to accommodate a set of (optional) PP-Modules.

3. Security Problem Definition

In this section, the security problem definition (SPD) for a DBMS is described. First, the informal discussion of the SPD is presented followed by a more formal description in terms of the identified threats, policies, and assumptions that will be used to identify the specific security requirements addressed by this cPP.

3.1 Informal Discussion

Given their common usage as repositories of high value data, attackers routinely target DBMS installations for compromise. Vulnerabilities that attackers may take advantage of are:

- Design flaws and programming bugs in the DBMS and the associated programs and systems, creating various security vulnerabilities (e.g. weak or ineffective access controls) which can lead to data loss/corruption, performance degradation etc;
- Unauthorized or unintended activity or misuse by authorized database users, or network/systems managers, or by unauthorized users or hackers (e.g. inappropriate access to sensitive data, metadata or functions within databases, or inappropriate changes to the database programs, structures or security configurations);
- Malware infections causing incidents such as unauthorized access, leakage or disclosure of personal or proprietary data, deletion of or damage to the data or programs, interruption or denial of authorized access to the database, attacks on other systems and the unanticipated failure of database services; and
- Data corruption and/or loss caused by the entry of invalid data or commands, mistakes in database or system administration processes, sabotage/criminal damage etc.

3.2 Assets and Threat Agents

The threats given in Section 3.3 refer to various threat agents and assets. The term "threat agent" is defined in CC Part 1.

The assets, mentioned in Table 1 below, are either defined in CC Part 1, or in the glossary which will be provided in the Appendix of the cPP document.

The terms "TSF data", "TSF" and "user data", are defined in CC Part 1. The terms "public objects" and "TOE resources" are given in the glossary which will be provided in the Appendix of the cPP document.

3.3 Threats

The following threats are identified and addressed by the TOE and should be read in conjunction with the threat rationale.

Compliant TOEs will provide security functionality that addresses threats to the TOE and implements policies that are imposed by the organization, law or regulation.

Table 1: Threats Applicable to the TOE

Threat	Definition
T.ACCESS_TSFDATA	A user or a process may read or modify TSF data using functions of the TOE without being identified, authenticated and authorized.
T.ACCESS_TSFFUNC	A user or a process may use, manage or modify the TSF, bypassing the protection mechanisms of the TSF.
T.IA_USER	A user who has not successfully completed identification and authentication may gain unauthorized access to user data or TOE resources beyond public objects.
T.RESIDUAL_DATA	A user or a process acting on behalf of a user may gain unauthorized access to user or TSF data through reallocation of TOE resources from one user or process to another.
T.UNAUTHORIZED_ACCESS	An authenticated user or a process, in conflict with the TOE security policy, may gain unauthorized access to user data.

3.4 Organizational Security Policies

The following organizational security policies are addressed by cPP-conformant TOEs:

Table 2: Policies Applicable to the TOE

Policy	Definition
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ROLES	Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible while supporting only the administrative duties the person has. This role shall be separate and distinct from other authorized users.
P.USER	Authority shall only be given to users who are trusted to perform the actions correctly and are permitted by the organization to access user data.

3.5 Assumptions

This section contains assumptions regarding the IT environment in which the TOE will reside.

Table 3: Assumptions Applicable to the TOE Environment

Assumption	Definition
Physical aspects	

A.PHYSICAL	The operational environment is assumed to provide the TOE with appropriate physical protection such that the TOE is not subject to physical attack that may compromise the security and/or interfere with the platform's correct operation. This includes protection for the physical infrastructure on which the TOE depends for correct operation and hardware devices on which the TOE is executing.
Personnel aspects	
A.AUTHUSER	Authorized users possess the necessary authorization to access the information managed by the TOE in accordance with organization information access policies.
A.MANAGE	The TOE security functionality is managed by one or more competent, authorized administrators. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.
A.TRAINEDUSER	Authorized users are sufficiently trained to accomplish a task or a group of tasks within a secure IT environment by exercising control over their user data.
Procedural aspects	
A.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration, and support of the DBMS.
A.PEER_FUNC_&_MGT	All external IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.
A.SUPPORT	Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is used by the TOE is correct and up to date.
Connectivity aspects	
A.CONNECT	All connections to and from remote trusted IT systems and between separate parts of the TSF are physically and/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.

4. Security Objectives

This section identifies the security objectives of the TOE and its supporting environment.

These security objectives identify the responsibilities of the TOE and its environment in meeting the security problem definition (SPD).

4.1 TOE security objectives

4.1.1 O.ADMIN_ROLE

The TOE shall provide roles that allow only authorized users to have access to administrative privileges that are specific to the role.

4.1.2 O.AUDIT_GENERATION

The TOE shall provide the capability to detect and create/generate records of security relevant events associated with users.

4.1.3 O.DISCRETIONARY_ACCESS

The TSF shall control access of subjects and/or users to named resources based on identity of the object, subject, or user. The TSF shall allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.

4.1.4 O.I&A

The TOE shall ensure that users are authenticated before the TOE processes any actions that require authentication.

4.1.5 O.MANAGE

The TSF shall provide all the functions and facilities necessary to manage TOE security mechanisms, and shall restrict such management actions to authorized users.

4.1.6 O.RESIDUAL_INFORMATION

The TOE shall ensure that any information contained in a protected resource within its control is not inappropriately disclosed when the resource is reallocated.

4.1.7 O.TOE_ACCESS

The TOE shall provide functionality that controls a user's logical access to user data and to the TSF.

4.2 Security Objectives for the Operational Environment

4.2.1 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.

4.2.2 OE.INFO_PROTECT

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

- All network and peripheral cabling shall be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques.
- DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly.
- Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.

4.2.3 OE.NO_GENERAL_ PURPOSE

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

4.2.4 OE.PHYSICAL

Those responsible for the TOE shall 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 shall be commensurate with the value of the IT assets protected by the TOE.

4.3 Security Objectives for the Operational IT Environment

4.3.1 OE.IT_I&A

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

4.3.2 OE.IT_TRUSTED_SYSTEM

External IT systems may be required by the TOE for the enforcement of the security policy. These external trusted IT systems shall be managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and are physically and shall be sufficiently protected from any attack that may cause those functions to provide false results.

5. Security Functional Requirements

The individual security functional requirements are specified in the sections below.

5.1 Class: Security Audit (FAU)

5.1.1 Audit Data Generation (FAU_GEN)

FAU_GEN.1 Audit data generation

FAU_GEN.1.1

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the minimum level of audit **listed in** Table 4: Auditable Events; and
c) [Start-up and shutdown of the DBMS; and
d) Use of special permissions (e.g., those often used by authorized administrators to circumvent access control policies).]

FAU_GEN.1.2

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, [information specified in column three of Table 4: Auditable Events, below].

Application Note 2: *In column 3 of the table below, "Additional Audit Record Contents" is used to designate data that should be included in the audit record if it "makes sense" in the context of the event which generates the record. If no other information is required (other than that listed in item a) above) for a particular auditable event type, then an assignment of "none" is acceptable.*

Table 4: Auditable Events

Column 1: Security Functional Requirement	**Column 2 Auditable Event(s)**	**Column 3 Additional Audit Record Contents**
FAU_GEN.1	None	None
FAU_GEN.2	None	None
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	The identity of the authorized administrator that made the change to the audit configuration
FDP_ACC.1	None	None

Column 1: Security Functional Requirement	Column 2 Auditable Event(s)	Column 3 Additional Audit Record Contents
FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP	None
FDP_RIP.1	None	None
FIA_ATD.1	None	None
FIA_UAU.2	Access denied by authentication mechanism	None
FIA_UID.2	Access denied by authentication mechanism	The user identity provided
FIA_USB_(EXT).2	Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject)	None
FMT_MSA.1	None	None
FMT_MSA.3	None	None
FMT_MTD.1	None	None
FMT_REV.1(1)	Unsuccessful revocation of security attributes	Identity of individual attempting to revoke security attributes
FMT_REV.1(2)	Unsuccessful revocation of security attributes	Identity of individual attempting to revoke security attributes
FMT_SMF.1	Use of the management functions	Identity of the administrator performing these functions
FMT_SMR.1	Modifications to the group of users that are part of a role	Identity of authorized administrator modifying the role definition
FPT_TRC.1	Restoring consistency	None
FTA_MCS.1	Rejection of a new session based on the limitation of multiple concurrent sessions	None
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism	Identity of the individual attempting to establish a session

FAU_GEN.2 User identity association

FAU_GEN.2.1

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

5.1.2 Security audit event selection (FAU_SEL)

FAU_SEL.1 Selective audit

FAU_SEL.1.1

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

a) user identity;

b) [selection: object identity, subject identity, host identity, **group identity,** event type**, success of auditable security events, failure of auditable security events**];

c) [assignment: list of additional attributes that audit selectivity is based upon].

Application Note 3: *"event type" is to be defined by the ST author; the intent is to be able to include or exclude classes of audit events.*

Application Note 4: *The intent of this requirement is to capture sufficient audit data to allow the administrators to perform their tasks; additional audit data may be captured.*

5.2 Class: User Data Protection (FDP)

5.2.1 Access control policy (FDP_ACC)

FDP_ACC.1 Subset access control

FDP_ACC.1.1

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

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1

The TSF shall enforce the [Discretionary Access Control policy] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

Application Note 5: *DBMS-controlled objects may be implementation-specific objects that are presented to authorized users at the user interface to the DBMS. They may include, but are not limited to tables, records, files, indexes, views, constraints, stored queries, and metadata. Data structures that are not presented to authorized users at the DBMS user interface, but are used internally, are internal TSF data structures. Internal TSF data structures are not controlled according to the rules specified in FDP_ACF.1.*

Application Note 6: *Named groups of security attributes can be specified to provide a convenient means to refer to multiple security attributes. In this PP, 'Named group of SFP-relevant security attributes' refers to a group of*

attributes that can be associated with an object or a subject. For example, this could be a named Access Control List (ACL).

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].

5.2.2 Residual information protection (FDP_RIP)

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1

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

5.3 Class: Identification and authentication (FIA)

Application Note 7: *It is drawn to the attention of the ST writer that the identification and authentication family was written in such a way that the SFRs might be used in either the case that Identification and Authentication (I&A) services are performed by the TOE itself or that they are performed within the TOE environment.*

5.3.1 User authentication (FIA_UAU)

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1

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

5.3.2 User attribute definition (FIA_ATD)

FIA_ATD.1 User attribute definition

FIA_ATD.1.1

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

a) [Database user identifier and any associated group memberships;
b) Security-relevant database roles; and
c) [assignment: list of security attributes]].

Application Note 8: *The intent of this requirement is to specify the TOE security attributes that the TOE utilizes to determine access. These attributes may be controlled by the environment or by the TOE itself.*

5.3.3 User identification (FIA_UID)

FIA_UID.2 User identification before any action

FIA_UID.2.1

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

5.4 Class: Security management (FMT)

5.4.1 FMT_MSA Management of security attributes

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1

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

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1

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

Application Note 9: *This requirement applies to new objects at the top-level (e.g., tables). When lower-level objects are created (e.g., rows, cells), these may inherit the permissions of the top-level objects by default. In other words, the permissions of the 'child' objects can take the permissions of the 'parent' objects by default.*

FMT_MSA.3.2

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

5.4.2 FMT_MTD Management of TSF data

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1

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

5.4.3 FMT_REV Revocation

FMT_REV.1(1) Revocation

FMT_REV.1.1(1)

The TSF shall restrict the ability to revoke [assignment: list of security attributes] associated with the *users* under the control of the TSF to [the authorized administrator].

FMT_REV.1.2(1)

The TSF shall enforce the rules [assignment: specification of revocation rules].

FMT_REV.1(2) Revocation (DAC)

FMT_REV.1.1(2)

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

FMT_REV.1.2(2)

The TSF shall enforce the rules [assignment: specification of revocation rules].

5.4.4 FMT_SMF Specification of management functions

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

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

- Database configuration
- User and role management

[selection:

- Management of groups
- Adding or removing a database
- Revocation of security attributes
- Configuration of the maximum number of concurrent sessions

- Configuration of session establishment rules
- Configuration of TSF replication and consistency
- Configuration of TOE access information rules
- No other security management functions]

[assignment: any additional security management functions required to configure the claimed security].

Application Note 10: *The ST author should ensure that all security attributes identified in FIA_ATD.1 are adequately managed and protected.*

5.4.5 FMT_SMR Security management roles

FMT_SMR.1 Security roles

FMT_SMR.1.1

The TSF shall maintain the roles [authorized administrator and [assignment: additional authorized identified roles]].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Application Note 11: *This requirement identifies a minimum set of management roles. An ST may describe, or an operational environment may contain a finer-grain decomposition of roles that correspond to the roles identified here (e.g., database non-administrative user or database operator). The ST author may change the names of the roles identified above but the "new" roles must still perform the functions that the security management requirements in this cPP have defined. It is not necessary to list roles that are not exercised in the evaluated configuration.*

5.5 Class: TOE access (FTA)

5.5.1 Limitation on multiple concurrent sessions (FTA_MCS)

FTA_MCS.1 Basic limitation on multiple concurrent sessions

FTA_MCS.1.1

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

FTA_MCS.1.2

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

Application Note 12: *The ST author is reminded that the CC part 2, [CC2] para 473 allows that the default number may be defined as a management function in FMT.*

5.5.2 TOE session establishment (FTA_TSE)

FTA_TSE.1 TOE session establishment

FTA_TSE.1.1

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

6. Security Assurance Requirements

The Security Objectives for the TOE in Section 4 were constructed to address threats identified in Section 3. The Security Functional Requirements (SFRs) in Section 5 are a formal instantiation of the Security Objectives. This cPP identifies the Security Assurance Requirements (SARs) to frame the extent to which the evaluator assesses the documentation applicable for the evaluation and performs independent testing.

This section lists the set of SARs from CC part 3 [CC3] that are required in evaluations against this cPP. Individual Evaluation Activities to be performed are specified in [SD].

The general model for evaluation of TOEs against STs written to conform to this cPP is as follows:

After the ST has been approved for evaluation, the IT Security Evaluation Facility (ITSEF) will obtain the TOE, supporting environmental IT (if required), and the administrative/user guides for the TOE. The ITSEF is expected to perform actions mandated by the Common Evaluation Methodology [CEM] for the ASE and ALC SARs. The ITSEF also performs the Evaluation Activities contained within the [SD], which are derived from the [CEM] assurance requirements as they apply to the specific technology instantiated in the TOE. The Evaluation Activities that are captured in the [SD] also provide clarification as to what the developer needs to provide to demonstrate the TOE is compliant with the cPP.

The TOE security assurance requirements are identified in Table 5.

Table 5: Security Assurance Requirements

Assurance Class	Assurance Components
Security Target (ASE)	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)
	Security objectives for the operational environment (ASE_OBJ.2)
	Stated security requirements (ASE_REQ.2)
	Security Problem Definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Security architecture description (ADV_ARC.1)
	Basic functional specification (ADV_FSP.2)
	Basic design (ADV_TDS.1)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life cycle support (ALC)	Labeling of the TOE (ALC_CMC.2)
	TOE CM coverage (ALC_CMS.2)
	Delivery procedures (ALC_DEL.1)
	Flaw reporting procedures (ALC_FLR.3)
Tests (ATE)	Evidence of coverage (ATE_COV.1)
	Functional testing (ATE_FUN.1)
	Independent testing – sample (ATE_IND.2)
Vulnerability assessment (AVA)	Vulnerability survey (AVA_VAN.2)

6.1 Class ASE: Security Target

NOTE: The Supporting Document [SD] contains evaluation activities that refine the evaluation activities given in [CEM].

6.2 Class ADV: Development

NOTE: The Supporting Document [SD] contains evaluation activities that refine the evaluation activities given in [CEM].

6.3 Class AGD: Guidance Documentation

NOTE: The Supporting Document [SD] contains evaluation activities that refine the evaluation activities given in [CEM].

6.4 Class ALC: Life-cycle Support

NOTE: The Supporting Document [SD] contains evaluation activities that refine the evaluation activities given in [CEM].

6.5 Class ATE: Tests

NOTE: The Supporting Document [SD] contains evaluation activities that refine the evaluation activities given in [CEM].

6.6 Class AVA: Vulnerability Assessment

NOTE: The Supporting Document [SD] contains evaluation activities that refine the evaluation activities given in [CEM].

A.Optional Requirements

As indicated in the introduction to this cPP, the baseline requirements (those that must be performed by the TOE) are contained in the body of this cPP. Additionally, there is another type of requirements specified in Appendix A

These requirements can be included in the ST, but do not have to be in order for a TOE to claim conformance to this cPP.

ST authors are free to choose none, some or all SFRs defined in this chapter. It is not a requirement to add the SFRs defined in this chapter, even if the functionality is supported by the product.

A.1 Class: Identification and authentication (FIA)

A.1.1 Enhanced user-subject binding (FIA_USB_EXT)

FIA_USB_EXT.2 Enhanced user-subject binding

FIA_USB_EXT.2 .1

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

FIA_USB_EXT.2 .2

The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: rules for the initial association of attributes].

FIA_USB_EXT.2 .3

The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: rules for the changing of attributes].

FIA_USB_EXT.2 .4

The TSF shall enforce the following rules for the assignment of subject security attributes not derived from user security attributes when a subject is created: [assignment: rules for the initial association of the subject security attributes not derived from user security attributes].

Application Note 13: *Some administrative tasks may be delegated to specific users (which by that delegation become administrators although they can only perform some limited administrative actions). Ensuring that those users*

cannot extend the administrative rights assigned to them is a security functionality the TOE has to provide.

A.2 Class: Protection of the TSF (FPT)

A.2.1 Internal TOE TSF data replication consistency (FPT_TRC)

FPT_TRC.1 Internal TSF consistency

FPT_TRC.1.1

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

FPT_TRC.1.2

When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [assignment: list of functions dependent on TSF data replication consistency].

Application Note 14: *In general, it is impossible to achieve complete, constant consistency of TSF data that is distributed to remote portions of a TOE because distributed portions of the TSF may be active at different times or disconnected from one another. This requirement attempts to address this situation in a practical manner by acknowledging that there will be TSF data inconsistencies but that they will be corrected without undue delay. For example, a TSF could provide timely consistency through periodic broadcast of TSF data to all TSF nodes maintaining replicated TSF data. Another example approach is for the TSF to provide a mechanism to explicitly probe remote TSF nodes for inconsistencies and respond with action to correct the identified inconsistencies.*

A.3 Class: TOE access (FTA)

A.3.1 TOE access information (FTA_TAH_EXT)

FTA_TAH_EXT.1 TOE access information

FTA_TAH_EXT.1.1

Upon a session establishment attempt, the TSF shall store

a) the [date and time] of the session establishment attempt of the user.
b) the incremental count of successive unsuccessful session establishment attempt(s).

FTA_TAH_EXT.1.2

Upon successful session establishment, the TSF shall allow the [date and time] of

a) the previous last successful session establishment, and

b) the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the previous last successful session establishment to be retrieved by the user.

Application Note 15: *If FTA_TAH_EXT.1 is included in an ST then Table 4: Auditable Events is refined to add the following entry:*

Column 1: Security Functional Requirement	**Column 2 Auditable Event(s)**	**Column 3 Additional Audit Record Contents**
FTA_TAH_EXT.1	None	None

B.Extended Component Definitions

This appendix contains the definitions for the extended requirements that are used in the cPP, including those used in Appendix A.

B.1 Class: User Identification and Authentication (FIA)

B.1.1 Enhanced user-subject binding (FIA_USB_EXT)

Family Behaviour

FIA_USB_EXT.2 is analogous to FIA_USB.1 except that it adds the possibility to specify rules whereby subject security attributes are also derived from TSF data other than user security attributes.

Component levelling

FIA_USB_EXT.2 is hierarchical to FIA_USB.1.

Management

See management description specified for FIA_USB.1 in [CC2].

Audit

See audit requirement specified for FIA_USB.1 in [CC2].

FIA_USB_EXT.2 Enhanced user-subject binding	
Hierarchical to:	FIA_USB.1 User-subject binding
Dependencies:	FIA_ATD.1 User attribute definition

FIA_USB_EXT.2.1

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

FIA_USB_EXT.2.2

The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: rules for the initial association of attributes].

FIA_USB_EXT.2.3

The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: rules for the changing of attributes].

FIA_USB_EXT.2.4

The TSF shall enforce the following rules for the assignment of subject security attributes not derived from user security attributes when a subject is created: [assignment: rules for the initial association of the subject security attributes not derived from user security attributes].

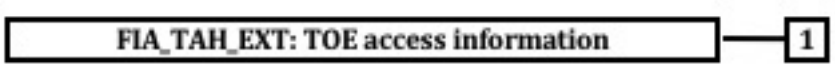
B.2 Class: TOE access (FTA)

B.2.1 TOE access information (FTA_TAH_EXT)

Family Behaviour

FTA_TAH_EXT.1 TOE access information provides the requirement for a TOE to make available information related to attempts to establish a session.

Component levelling



FTA_TAH_EXT.1 is not hierarchical to any other components.

Management:

There are no management activities foreseen.

Audit:

There are no auditable events foreseen.

FTA_TAH_EXT.1 TOE access information
Hierarchical to: No other components.
Dependencies: No dependencies.

FTA_TAH_EXT.1.1

Upon a session establishment attempt, the TSF shall store

a) the [date and time] of the session establishment attempt of the user.
b) the incremental count of successive unsuccessful session establishment attempt(s).

FTA_TAH_EXT.1.2

Upon successful session establishment, the TSF shall allow the [date and time] of

a) the previous last successful session establishment, and
b) the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the previous last successful session establishment

to be retrieved by the user.

C. Rationales

C.1 TOE Security Objectives Coverage

The table below gives a summary of the policies, and threats relating to the TOE security objectives.

Table 6: Coverage of Security Objectives for the TOE

Objective Name	SPD coverage
O.ADMIN_ROLE	P.ACCOUNTABILITY P.ROLES T.ACCESS_TSFFUNC
O.AUDIT_GENERATION	P.ACCOUNTABILITY
O.DISCRETIONARY_ACCESS	T.IA_USER T.UNAUTHORIZED_ACCESS
O.I&A	P.ACCOUNTABILITY T.ACCESS_TSFFUNC T.ACCESS_TSFDATA T.IA_USER
O.MANAGE	P.USER T.ACCESS_TSFDATA T.ACCESS_TSFFUNC T.UNAUTHORIZED_ACCESS
O.RESIDUAL_INFORMATION	T.RESIDUAL_DATA
O.TOE_ACCESS	P.ACCOUNTABILITY P.ROLES P.USER T.ACCESS_TSFDATA T.ACCESS_TSFFUNC T.IA_USER T.UNAUTHORIZED_ACCESS

C.2 Rationale for TOE Security Objectives

The table below gives the rationale for the TOE security objectives.

Table 7: Rationale for the TOE Security Objectives

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE.	O.ADMIN_ROLE The TOE shall provide roles that allow only authorized users to have access to administrative privileges that are specific to the role.	O.ADMIN_ROLE supports this policy by ensuring that the TOE provides a means of granting authorized administrators the privileges needed for secure administration.
	O.AUDIT_GENERATION The TOE shall provide the capability to generate records of security relevant events associated with users.	O.AUDIT_GENERATION supports this policy by ensuring that audit records are generated to enable accountability.
	O.I&A The TOE shall ensure that users are authenticated before the TOE processes any actions that require authentication.	O.I&A supports this policy by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action.
	O.TOE_ACCESS The TOE shall provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS supports this policy by providing a mechanism for controlling user access.

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
P.USER Authority shall only be given to users who are trusted to perform the actions correctly and are permitted by the organization to access user data.	O.MANAGE The TSF shall provide all the functions and facilities necessary to manage TOE security mechanisms, and shall restrict such management actions to authorized users.	O.MANAGE supports this policy by ensuring that the functions and facilities supporting secure management are in place.
	O.TOE_ACCESS The TOE shall provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS supports this policy by providing a mechanism for controlling user access.
	OE.ADMIN Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and ensuring the security of information it contains.	OE.ADMIN supports this policy by ensuring that only competent administrators are allowed to manage the TOE.

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
P.ROLES Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible while supporting only the administrative duties the person has. This role shall be separate and distinct from other authorized users.	O.ADMIN_ROLE The TOE shall provide roles that allow only authorized users to have access to administrative privileges that are specific to the role.	O.ADMIN_ROLE supports this objective by providing roles that allow only authorized users access to administrative privileges.
	O.TOE_ACCESS The TOE shall provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS supports this policy by controlling access to TSF functionality based on role.

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
T.ACCESS _TSFDATA A user or a process may read or modify TSF data using functions of the TOE without being identified, authenticated and authorized.	O.I&A The TOE shall ensure that users are authenticated before the TOE processes any actions that require authentication.	O.I&A supports this policy by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE is defined to provide to authenticated users only.
	O.MANAGE The TSF shall provide all the functions and facilities necessary to manage TOE security mechanisms, and shall restrict such management actions to authorized users.	O.MANAGE diminishes this threat since it ensures that functions and facilities used to modify TSF data are not available to unauthorized users.
	O.TOE_ACCESS The TOE shall provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS mitigates this threat by restricting TOE access.

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
T.ACCESS _TSFFUNC A user or a process may use, manage or modify the TSF, bypassing the protection mechanisms of the TSF.	O.ADMIN_ROLE The TOE will provide roles that allow only authorized users to have access to administrative privileges that are specific to the role.	O.ADMIN_ROLE mitigates this threat by restricting access to privileged actions.
	O.I&A The TOE shall ensure that users are authenticated before the TOE processes any actions that require authentication.	O.I&A mitigates this threat since the TOE requires successful authentication to the TOE prior to gaining access to any controlled-access content.
	O.MANAGE The TSF shall provide all the functions and facilities necessary to manage TOE security mechanisms, and shall restrict such management actions to authorized users.	O.MANAGE mitigates this threat by ensuring that management functions are restricted to authorized users.
	O.TOE_ACCESS The TOE shall provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS mitigates this threat by restricting TOE access.

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
T.IA_USER A user who has not successfully completed identification and authentication may gain unauthorized access to user data or TOE resources beyond public objects.	O.DISCRETIONARY_ACCESS The TSF shall control access of subjects and/or users to named resources based on identity of the object, subject, or user. The TSF shall 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.DISCRETIONARY_ACCESS mitigates this threat by requiring that data, including user data stored with the TOE, is protected by discretionary access controls.
	O.I&A The TOE shall ensure that users are authenticated before the TOE processes any actions that require authentication.	O.I&A mitigates this threat by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing access beyond public objects.
	O.TOE_ACCESS The TOE shall provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS mitigates this threat by controlling logical access to user data and TSF data.

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
T.RESIDUAL_DATA A user or a process acting on behalf of a user may gain unauthorized access to user or TSF data through reallocation of TOE resources from one user or process to another.	O.RESIDUAL_INFORMATION The TOE shall ensure that any information contained in a protected resource is not inappropriately disclosed when the resource is reallocated.	O.RESIDUAL_INFORMATION mitigates this threat by ensuring that data is not improperly disclosed.

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
T.UNAUTHORIZED_ACCESS An authenticated user or a process, in conflict with the TOE security policy, may gain unauthorized access to user data.	O.DISCRETIONARY_ACCESS The TSF shall control access of subjects and/or users to named resources based on identity of the object, subject or user. The TSF shall 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.DISCRETIONARY_ACCESS mitigates this threat by requiring that data, including TSF data, is protected by discretionary access controls.
	O.MANAGE The TSF shall provide all the functions and facilities necessary to manage TOE security mechanisms, and shall restrict such management actions to authorized users.	O.MANAGE mitigates this threat by ensuring that access to user data is restricted to authorized users.
	O.TOE_ACCESS The TOE shall provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS mitigates this threat by controlling logical access to user data and TSF data.

C.3 Rationale for the Environmental Security Objectives

The table below gives a summary of the assumptions, policies, and threats relating to the environmental security objectives.

Table 8: Coverage of SPF Items for the TOE Environment Security Objectives

Objective Name	SPD coverage
OE.ADMIN	A.MANAGE P.USER
OE.INFO_PROTECT	A.AUTHUSER A.CONNECT A.MANAGE A.PHYSICAL A.TRAINEDUSER P.USER T.UNAUTHORIZED_ACCESS
OE.IT_I&A	A.SUPPORT
OE.IT_TRUSTED_SYSTEM	A.CONNECT A.PEER_FUNC_&_MGT
OE.NO_GENERAL_ PURPOSE	A.NO_GENERAL_PURPOSE
OE.PHYSICAL	A.CONNECT A.PHYSICAL

The table below provides a rationale for the environmental security objectives.

Table 9: Rationale for Environmental Security Objectives

Assumption	Environmental Objective Addressing the Assumption	Rationale for Specifying the Environmental Security Objective
A.AUTHUSER Authorized users possess the necessary authorization to access the information managed by the TOE in accordance with organization information access policies.	OE.INFO_PROTECT Those responsible for the TOE shall establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling shall be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT supports the assumption by ensuring that users are authorized to access data managed by the TOE.

Assumption	Environmental Objective Addressing the Assumption	Rationale for Specifying the Environmental Security Objective
A.CONNECT All connections to and from remote trusted IT systems and between separate parts of the TSF are physically and/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.	OE.INFO_PROTECT Those responsible for the TOE shall establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling shall be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT supports the assumption by requiring that all network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques.
	OE.IT_TRUSTED_SYSTEM External IT systems may be required by the TOE for the enforcement of the security policy. These external trusted IT systems shall be managed according to known, accepted and trusted policies based on the same rules and policies applicable to the TOE, and shall be sufficiently protected from any attack that may cause those functions to provide false results.	OE.IT_TRUSTED_SYSTEM supports the assumption by ensuring that external trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy.
	OE.PHYSICAL Those responsible for the TOE shall 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 shall be commensurate with the value of the IT assets protected by the TOE.	OE.PHYSICAL supports the assumption by ensuring that appropriate physical security is provided within the domain.

Assumption	Environmental Objective Addressing the Assumption	Rationale for Specifying the Environmental Security Objective
A.SUPPORT Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is used by the TOE is correct and up to date.	OE.IT_I&A Any information provided by a trusted entity in the environment and used to support user authentication and authorization used by the TOE is correct and up to date.	OE.IT_I&A supports the assumption implicitly.
A.MANAGE The TOE security functionality is managed by one or more competent, authorized administrators. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.	OE.ADMIN Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of information it contains.	OE.ADMIN supports the assumption by requiring that authorized administrators are competent, thereby ensuring that all the tasks are performed correctly and effectively.
	OE.INFO_PROTECT Those responsible for the TOE shall establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling shall be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and 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.INFO_PROTECT supports the assumption by ensuring that users are authorized to access the appropriate data, and are trained to exercise control.

Assumption	Environmental Objective Addressing the Assumption	Rationale for Specifying the Environmental Security Objective
A.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration, and support of the DBMS.	OE.NO_GENERAL_PURPOSE There shall be no general-purpose computing capabilities (e.g., compilers or user applications) available on DMBS servers, other than those services necessary for the operation, administration, and support of the DBMS.	OE.NO_GENERAL_PURPOSE The DBMS server must not include any general-purpose computing capabilities. This will protect the TSF data from malicious processes.
A.PEER_FUNC_&_MGT All external trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.	OE.IT_TRUSTED_SYSTEM External IT systems may be required by the TOE for the enforcement of the security policy. These external trusted IT systems shall be managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and shall be sufficiently protected from any attack that may cause those functions to provide false results.	OE.IT_TRUSTED_SYSTEM supports this assumption by ensuring that remote systems supporting the TOE are managed in a manner consistent with the security policies applicable to the TOE.

Assumption	Environmental Objective Addressing the Assumption	Rationale for Specifying the Environmental Security Objective
A.PHYSICAL The operational environment is assumed to provide the TOE with appropriate physical protection such that the TOE is not subject to physical attack that may compromise the security and/or interfere with the platform's correct operation. This includes protection for the physical infrastructure on which the TOE depends for correct operation and hardware devices on which the TOE is executing.	OE.PHYSICAL Those responsible for the TOE shall 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 shall be commensurate with the value of the IT assets protected by the TOE.	OE.PHYSICAL supports this assumption by ensuring that the parts of the TOE critical to the enforcement of the security policy are protected from physical attack.
	OE.INFO_PROTECT Those responsible for the TOE shall establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling shall be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and 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.INFO_PROTECT supports the assumption by requiring that all network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques.

Assumption	Environmental Objective Addressing the Assumption	Rationale for Specifying the Environmental Security Objective
A.TRAINEDUSER Authorized users are sufficiently trained to accomplish a task or group of tasks within a secure IT environment by exercising control over their user data.	OE.INFO_PROTECT Those responsible for the TOE shall establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling shall be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and 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.INFO_PROTECT supports the assumption by ensuring that users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.

Assumption	Environmental Objective Addressing the Assumption	Rationale for Specifying the Environmental Security Objective
P.USER Authority shall only be given to users who are trusted to perform the actions correctly.	OE.ADMIN Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of information it contains.	OE.ADMIN supports the policy by ensuring that the authorized administrators, responsible for granting authority to users, are trustworthy.
	OE.INFO_PROTECT Those responsible for the TOE shall establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling shall be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT supports the policy by ensuring that users are authorized to access parts of the data managed by the TOE.

Assumption	Environmental Objective Addressing the Assumption	Rationale for Specifying the Environmental Security Objective
T.UNAUTHORIZED _ACCESS A user may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.	OE.INFO_PROTECT Those responsible for the TOE shall establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling shall be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT diminishes the logical and physical threats by ensuring that the network and peripheral cabling are appropriately protected. DAC protections, when implemented correctly, support the identification of unauthorized access.

C.4 Rationale for TOE Security Functional Requirements

The following table provides the rationale for the selection of the security functional requirements. It traces each TOE security objective to the identified security functional requirements.

Table 10: Rationale for TOE Security Functional Requirements

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN_ROLE The TOE shall provide roles that allow only authorized users to have access to administrative privileges that are specific to the role.	FMT_SMR.1	The TOE will establish, at least, an authorized administrator role. Additional roles may also be specified.

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT_GENERATION The TOE shall provide the capability to detect and create records of security relevant events associated with users.	FAU_GEN.1 FAU_GEN.2 FAU_SEL.1	FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that the administrator has the ability to audit any security relevant events that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. FAU_GEN.2 ensures that the audit records associate a user and any associated group identity with the auditable event. FAU_SEL.1 allows the administrator to configure which auditable events will be recorded in the audit trail.
O.DISCRETIONARY_ACCESS The TSF shall control access of subjects and/or users to named resources based on identity of the object, subject or user. The TSF shall allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.	FDP_ACC.1 FDP_ACF.1	The TSF controls access to resources based on the subject and/or object security attributes.
O.I&A The TOE shall ensure that users are authenticated before the TOE processes any actions that require authentication.	FIA_ATD.1 FIA_UAU.2 FIA_UID.2 FIA_USB_(EXT).2 (Optional)	FIA_UID.2 and FIA_UAU.2ensure that only authorized users gain access to the TOE and its resources following identification and authentication. FIA_ATD.1 ensures that the security attributes used to determine access are defined and available to the support access control decisions. FIA_USB_(EXT).2 ensures enforcement of the rules governing subjects acting on behalf of authorized users.

Objective	Requirements Addressing the Objective	Rationale
O.MANAGE The TSF shall provide all the functions and facilities necessary to manage TOE security mechanisms, and shall restrict such management actions to authorized users.	FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_REV.1(1) FMT_REV.1(2) FMT_SMF.1 FMT_SMR.1	FMT_MSA.1 ensures that the ability to perform operations on security attributes is restricted to authorized administrators. FMT_MSA.3 ensures that default values used for security attributes are restrictive. FMT_MTD.1 ensures that the ability to include or exclude auditable events is restricted to authorized administrators. FMT_REV.1 restricts the ability to revoke attributes to the authorized administrator. FMT_SMF.1 identifies the management functions that are available to the authorized administrator. FMT_SMR.1 defines the specific security roles to be supported.
O.RESIDUAL_INFORMATION The TOE shall ensure that any information contained in a protected resource within its control is not inappropriately disclosed when the resource is reallocated.	FDP_RIP.1	FDP_RIP.1 ensures that the contents of resources are not available upon reallocation of the resource.

Objective	Requirements Addressing the Objective	Rationale
O.TOE_ACCESS The TOE shall provide mechanisms that control a user's logical access to user data and to the TSF.	FDP_ACC.1 FDP_ACF.1 FIA_ATD.1 FTA_MCS.1 FTA_TSE.1 FTA_TAH_EXT.1 (Optional) FPT_TRC.1 (Optional)	FDP_ACC.1 and FDP_ACF.1 ensure that access between subjects and objects is controlled using security attributes. FIA_ATD.1 defines the security attributes for individual users. FTA_MCS.1 ensures that users are restricted to no more than a specified number of concurrent sessions. FTA_TSE.1 allows the TOE to restrict access to the TOE based on specified criteria. FTA_TAH_EXT.1 The TOE must be able to store and retrieve information about previous unauthorized login attempts and the number of times the login was attempted every time the user logs into their account. The TOE must also store the last successful authorized login. This information will include the date, time, method, and location of the attempts. Access to this data is controlled and restricted such that a user may only access his or her own data. FPT_TRC.1 If included in an ST, FPT_TRC.1 ensures replicated TSF data that specifies attributes for access control must be consistent across distributed components of the TOE. The requirement is to maintain consistency of replicated TSF data and associated access controls.

C.5 SFR Dependencies Analysis

Requirement	Dependency	Satisfied
FAU_GEN.1	FPT_STM.1	This requirement is satisfied by the assumption on the IT environment, given in A.SUPPORT.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	This requirement is satisfied by FAU_GEN.1. This requirement is satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1.
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	This requirement is satisfied by FAU_GEN.1. This requirement is satisfied by FMT_MTD.1.
FDP_ACC.1	FDP_ACF.1	This requirement is satisfied by FDP_ACF.1.
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	This requirement is satisfied by FDP_ACC.1. This requirement is satisfied by FMT_MSA.3.
FDP_RIP.1	None	N/A
FIA_ATD.1	None	N/A
FIA_UAU.2	FIA_UID.1	This requirement is satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1.
FIA_UID.2	None	N/A
FIA_USB_(EXT).2	FIA_ATD.1	This requirement is satisfied by FIA_ATD.1.
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	This requirement is satisfied by FDP_ACC.1. This requirement is satisfied by FMT_SMF.1. This requirement is satisfied by FMT_SMR.1.
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	This requirement is satisfied by FMT_MSA.1. This requirement is satisfied by FMT_SMR.1.
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	This requirement is satisfied by FMT_SMF.1. This requirement is satisfied by FMT_SMR.1.
FMT_REV.1(1)	FMT_SMR.1	This requirement is satisfied by FMT_SMR.1.
FMT_REV.1(2)	FMT_SMR.1	This requirement is satisfied by FMT_SMR.1.
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	This requirement is satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1.

Requirement	Dependency	Satisfied
FPT_TRC.1	FPT_ITT.1	For a distributed TOE, the dependency is satisfied through the environmental assumption, A.CONNECT, that assures the confidentiality and integrity of the transmitted data.
FTA_MCS.1	FIA_UID.1	This requirement is satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1.
FTA_TSE.1	None	N/A

C.6 SAR Dependencies Analysis

C.7 Rationale for Extended Security Functional Requirements

The table below presents a rationale for the inclusion of the extended functional security requirements found in this PP. Note that there are no extended security assurance requirements (SAR).

Table 11: Rationale for Extended Security Functional Requirements

Extended Requirement	Identifier	Rationale
FIA_USB_EXT.2	Enhanced user-subject binding	Security attributes may be associated with a user to further restrict access or provide additional privileges.
FTA_TAH_EXT.2	TOE access information	The TOE may make information related to attempts to establish a session available to users.

Glossary

The terms, definitions and abbreviations given [CC1] apply to this document. Additional terms, definitions and abbreviations applicable only within the DBMS cPP context are given below:

Terms and Definitions

Term	Meaning
Access	Interaction between an entity and an object that results in the flow or modification of data.
Access Control	Security service that controls the use of resources[2] and the disclosure and modification of data.[3]
Accountability	Property that allows activities in an IT system to be traced to the entity responsible for the activity.
Administrator	A user who has been specifically granted the authority to manage some portion or the entire TOE and whose actions may affect the DAC. Administrators may possess special privileges that provide capabilities to override portions of the access control policy.
Application	An executable program.
Assurance	A measure of confidence that the security features of an IT system are sufficient to enforce its security policy.
Attack	An intentional act attempting to violate the security policy of an IT system.
Authentication	Security measure that verifies a claimed identity.
Authorization	Permission, granted by an entity authorized to do so, to perform functions and access data.
Authorized Administrator	The authorized person in contact with the Target of Evaluation who is responsible for maintaining its operational capability.
Authorized User	An authenticated user who may, in accordance with the access control policy, perform an operation.
Availability	Timely[4], reliable access to IT resources.
Compromise	Violation of a security policy.
Confidentiality	A security policy pertaining to the disclosure of data.
Database Management System (DBMS)	A suite of programs that typically manage large structured sets of persistent data, offering ad hoc query facilities to many users. They are widely used in business applications.

[2] Hardware and software

[3] Stored or communicated

[4] According to a defined metric

Term	Meaning
Discretionary Access Control (DAC)	A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. Those controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.
Entity	A subject, object, user or another IT device, which interacts with TOE objects, data, or resources.
External IT entity	Any trusted Information Technology (IT) product or system, outside of the TOE, which may, in accordance with the access control policy, perform an operation.
Group	A group is a defined set. It is often used to describe a defined set of users.
Identity	A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Integrity	A security policy pertaining to the corruption of data and TSF mechanisms.
Named Object	An object that exhibits all of the following characteristics: • The object may be used to transfer information between subjects of differing user and/or group identities within the TSF. • Subjects in the TOE must be able to require a specific instance of the object. • The name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with different user and/or group identities to require the same instance of the object.
Object	An entity that contains or receives information and upon which subjects perform operations.
Platform	The environment in which application software runs. The platform can be an operating system, an execution environment which runs atop an operating system, or some combination of these.
Public Object	An object for which the TSF unconditionally permits all entities “read” access. Only the TSF or authorized administrators may create, delete, or modify the public objects.
Security attributes	TSF data associated with subjects, objects, and users that are used for the enforcement of the DAC policy.
Subject	An entity that causes operation to be performed.
Threat	Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.
TOE resources	Anything useable or consumable in the TOE.
Unauthorized user	A user who may obtain access only to system provided public objects if any exist.

Term	Meaning
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Vulnerability	A weakness that can be exploited to violate the TOE security policy.

Acronyms used in this cPP

Acronym	Meaning
ACL	Access Control List
CC	Common Criteria
COTS	Commercial Off The Shelf
DAC	Discretionary Access Control
DBMS	Database Management System
DBMS cPP	Database Management System collaborative Protection Profile
I&A	Identification and Authentication
IT	Information Technology
ITSEF	IT Security Evaluation Facility
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SPD	Security Problem Definition
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interfaces