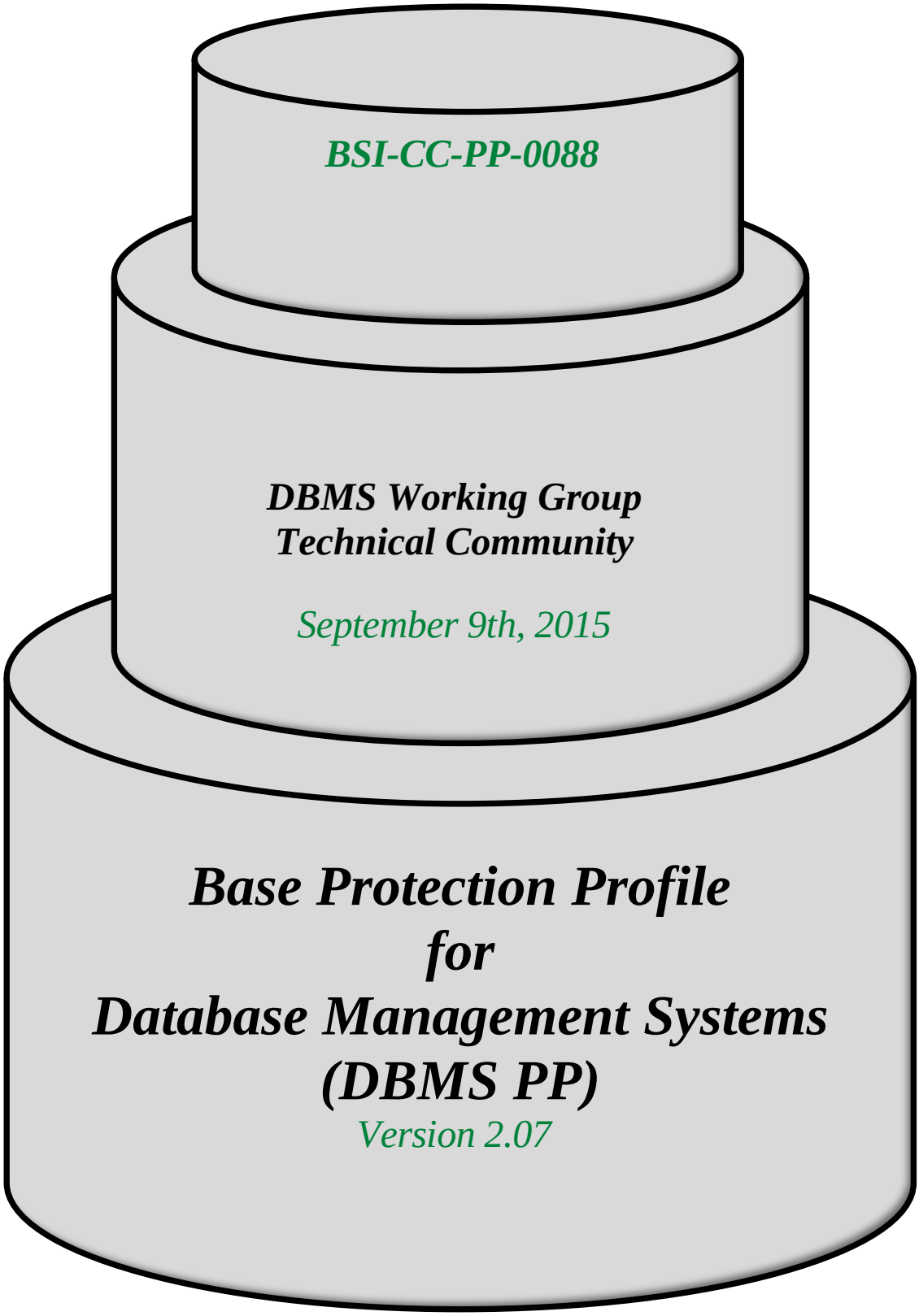
BSI-CC-PP-0088
DBMS Working Group
Technical Community
September 9th, 2015
Base Protection Profile
for
Database Management Systems
(DBMS PP)
Version 2.07

Revision History

Version	Date	Description
1.0	September 30, 2004	U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments BR-DBMSPP
1.1	June 7, 2006	U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments BR-DBMSPP
1.2	July 25, 2007	U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments BR-DBMSPP
1.3	December 24, 2010	U.S. Government Protection Profile for Database Management Systems DBMSPP
2.0	December 15, 2014	Base Protection Profile for Database Management Systems DBMS PP
2.07	September 9th, 2015	Certified Version of Base Protection Profile for Database Management Systems DBMS PP

Further information, including the status and updates of this protection profile can be found in the DBMS WG/TC project area on the CCUF website:
https://ccusersforum.onlyoffice.com/products/projects/tasks.aspx?prjID=410822

Comments on this document should be submitted to the DBMS WG/TC workspace. The comment should include the title and version of the document, the page, the section number, the line number, and the detailed comment and recommendation.

Protection Profile Title:

Base Protection Profile for Database Management Systems

Common Criteria Version:

This Protection Profile "Base Protection Profile for Database Management Systems" (DBMS PP) was updated using Version 3.1 of the Common Criteria (CC) [REF 1].

Table of Contents

List of Tables

1 INTRODUCTION TO THE PROTECTION PROFILE

1.1 PP Identification

Title: Base Protection Profile for Database Management Systems (DBMS PP)

Sponsor: DBMS Working Group / Technical Community

CC Version: Common Criteria (CC) Version 3.1 [REF 1]

PP Version: 2.07

Publication Date: 9th September, 2015

Keywords: database management system, DBMS PP, DBMS, COTS, commercial security, access control, CC EAL2 augmented.

1.2 TOE Overview

The "Base Protection Profile for Database Management Systems" specifies security requirements for a commercial-off-the-shelf (COTS) database management system (DBMS). The TOE type is a database management system.

A TOE compliant with this Protection Profile 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., operating system, 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.

Security Targets (STs) that claim conformance to this PP shall meet a minimum standard of demonstrable-PP conformance as defined in section D3 of Part 1 of the CC. [REF 1a]

1.3 PP Configurations

The Protection Profile for Database Management Systems (DBMS PP) is structured as a Base Protection Profile, ready to accommodate a set of (optional) Protection Profile extended packages[1]. This structure was chosen to maximize adaptability for different operational environments and different operational requirements, since Database Management Systems may provide functionality in a variety of ways.

The following PP configuration is allowed:

[1] These are also known as "Protection Profile modules". Please see [REF 2] for more details.

1. Base PP only (DBMS PP)

1.4 Document Conventions

Except for replacing United Kingdom spelling with American spelling, the notation, formatting, and conventions used in this PP are consistent with version 3.1 of the CC. Selected presentation choices are discussed here to aid the PP 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 [REF 1a]. Each of these operations is used in this 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 PP 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 and security target 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 PP, 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.

1.5 Glossary of Terms

See Appendix B for the Glossary of Terms.

1.6 Document Organization

Section 1 provides the introductory material for the protection profile.

Section 2 describes the Target of Evaluation in terms of its envisaged usage and connectivity.

Section 3 gives the conformance claims made by this protection profile.

Section 4 defines the security problem in terms of threats and security problems.

Section 5 identifies the security objectives derived from these threats and policies.

Section 6 identifies and defines the extended security requirements.

Section 7 identifies and defines the security functional requirements from the CC that must be met by the TOE in order for the functionality-based objectives to be met. This section also identifies the security assurance requirements for evaluation security level (EAL) 2 augmented.

Section 8 provides a rationale to demonstrate that the Information Technology Security Objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirement. Arguments are provided for the coverage of each objective.

Section 9, Appendices, includes the appendices that accompany the PP and provides clarity and/or explanation for the reader.

> Appendix A, References, provides background material for further investigation by users of the PP.
>
> Appendix B, Glossary, provides a listing of definitions of terms.
>
> Appendix C, Abbreviations and Acronyms, provides a listing of abbreviations and acronyms used throughout the document.

2 TOE DESCRIPTION

2.1 Product Type

The product type of the Target of Evaluation (TOE) described in this Protection Profile (PP) is a database management system (DBMS).

A DBMS is a computerized repository that stores information and allows authorized users to retrieve and update that information. 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 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.

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

a) Controlling users' accesses to user data and DBMS data;

b) Interacting with, and possibly supplementing portions of, the underlying operating system to retrieve and present the data that are under the DBMS's management;

c) Indexing data values to their physical locations for quick retrievals based on a value or range of values;

d) Executing pre-written programs (i.e., utilities) to perform common tasks like database backup, recovery, loading, and copying;

e) Supporting mechanisms that enable concurrent database access (e.g., locks);

f) Assisting recovery of user data and DBMS data (e.g., transaction log); and

g) 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 major types of users:

- Users who interact with the DBMS to observe and/or modify data objects for which they

have authorization to access; and

- 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:

- 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.

- 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.

2.2 TOE Definition

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

This PP does not dictate a specific architecture. The ST writer will need to identify and describe the TOE architecture to be evaluated.

The external IT entities, with which the DBMS may interact, if they are outside the TOE, 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, audit servers, and transaction processors with which the DBMS may interact to perform a DBMS function or a security function.

If the host OS is outside the TOE, 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. However, the goals of confidentiality, integrity, and availability for the TOE must be met by the total package: the DBMS and the external IT entities with which it interacts. In all cases, the TOE must be installed and administered in accordance with the TOE installation and administration instructions.

2.3 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.

  NOTE: 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.

2.4 Optional Security Functionality

Security services that must be provided either by the TOE and/or by the IT environment.

This security functionality is not modeled in the following chapters of the DBMS Base PP. The ST author must integrate the description of the additional (optional) security functionality and the corresponding security functional requirements.

- Identification and Authentication (I&A) by which users are uniquely identified and authenticated before they are authorized to access information stored on the DBMS.

- Audit Storage service that stores records for all security-relevant operations that users perform on user and DBMS data.

- Audit Review service that allows the authorized administrator to review stored audit records in order to detect potential and actual security violations.

However, compliance with this PP 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 a hacker attack 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.

2.5 TOE Operational Environment

2.5.1 Enclave

The term "enclave" further characterizes the environment in which the TOE is intended to operate. An enclave is under the control of a single authority and has a homogeneous security policy, including personnel and physical security, to protect it from other environments. An enclave can be specific to an organization or a mission and it may contain multiple networks. Enclaves may be logical, such as an operational area network, or be based on physical location and proximity. Any local and external elements that access resources within the enclave must satisfy the policy of the enclave.

The DBMS is expected to interact with other IT products that reside in the host OS, in the IT environment in which the host computer and host OS reside, and outside that environment but inside the enclave. The IT and non-IT mechanisms used for secure exchanges of information between the DBMS and such products are expected to be administratively determined and coordinated. Similarly, the IT and non-IT mechanisms for negotiating or translating the DAC policy involved in such exchanges are expected to be resolved by the organizations involved.

The DBMS may also interact with IT products outside the enclave such as a certificate authority (CA) that is defined as a trusted CA by an IT product within the enclave.

2.5.2 TOE Architectures

This PP does not dictate a specific architecture. A TOE compliant with this PP 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;

- 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); and

- A network of workstations communicating with several distributed DBMS servers simultaneously; the DBMS servers may all be within a single local area network, or they may be distributed geographically.

This PP allows each of these architectures to be supported as well as others. A possible architecture is an enclave in which DBMS users access the TOE via a local area network (LAN). Users in other enclaves will access the LAN and the host computers and servers on it by way of one or more boundary protection mechanisms (e.g., a firewall) and then through a communications server or router to the LAN. Depending on the particular enclave configuration and the DBMS access policy that it supports, all users (both inside and outside the enclave) may then access an application server, which either connects the TOE user to the enclave computer on which the TOE operates or manages the complete user/DBMS session.

2.5.3 TOE Administration

This PP defines one necessary administrator role (authorized administrator) which is established by the developer of the DBMS. This PP allows the DBMS developer or security target writer to define more 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. Of course, the very ability to establish and assign privileges will itself be a privileged function.

3 CONFORMANCE CLAIMS

The following sections describe the conformance claims of the Database Management System Protection Profile (DBMS PP).

3.1 Conformance with CC parts 2 and 3

DBMS PP is CC version 3.1 revision 4 Part 2 extended and Part 3 conformant.

3.2 Conformance with Packages

The DBMS PP claims an evaluation assurance level of EAL2 augmented by ALC_FLR.2.

3.3 Conformance with other Protection Profiles

DBMS PP does not claim conformance to any other Protection Profile.

3.4 Conformance Statement

DBMS PP requires demonstrable conformance by an ST.

4 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 PP.

4.1 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

- 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.

4.2 Assets and Threat Agents

The threats given in Section 4.3 refer to various threat agents and assets. The term "threat agent" is defined in CC Part 1. The term "A user or a process acting on behalf of a user" used in this PP, specifies a particular class of entities that can adversely act on assets.

The assets, mentioned in Table 1 below are either defined in CC part 1 [REF 1a], or in the glossary given in Appendix B of this document.

The terms "TSF data", "TSF" and "user data", are defined in CC Part 1. The terms "executable code within the TSF", " public objects ", "TOE resources" and "configuration data" are given in the glossary given in Appendix B of this document:

4.3 Threats

The following threats are identified and addressed by the TOE, and should be read in conjunction with the threat rationale, in Section 8.1.

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

Table 1: Threats Applicable to the TOE

Threat	Definition
T.ACCESS_TSFDATA	A threat agent may read or modify TSF data using functions of the TOE without the proper authorization.
T.ACCESS_TSFFUNC	A threat agent may use or manage TSF, bypassing the protection mechanisms of the TSF.
T.IA_MASQUERADE	A user or a process acting on behalf of a user may masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources.
T.IA_USER	A threat agent may gain access to user data, TSF data, or TOE resources with the exception of public objects without being identified and authenticated.
T.RESIDUAL_DATA	A user or a process acting on behalf of a user may gain unauthorized access to user or TSF data through reallocation of TOE resources from one user or process to another.
T.TSF_COMPROMISE	A user or a process acting on behalf of a use may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable code within the TSF.
T.UNAUTHORIZED_ACCESS	A threat agent may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.

4.4 Organizational Security Policies

The following organizational security policies are addressed by PP-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 supporting only the administrative duties the person has. This role shall be separate and distinct from other authorized users.
P.USER	Authority shall only be given to users who are trusted to perform the actions correctly.

4.5 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	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.
Personnel aspects	
A.AUTHUSER	Authorized users possess the necessary authorization to access at least some of the information managed by the TOE.
A.MANAGE	The TOE security functionality is managed by one or more competent 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	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.
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 remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.
A.SUPPORT	Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is used by the TOE is correct and up to date.
Connectivity aspects	
A.CONNECT	All connections to and from remote trusted IT systems and between separate parts of the TSF are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points. *Application Note: If the TOE consists of separate parts and the TOE implements mechanisms ensuring the protection of TSF data in transit between these parts, the ST author may consider claiming FPT_ITT.1 to supplement or replace A.CONNECT.*

5 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).

5.1 TOE Security Objectives

Table 4: TOE Security Objectives

Objective Name	Objective Definition
O.ACCESS_HISTORY	The TOE will store information related to previous attempts to establish a session and make that information available to the user.
O.ADMIN_ROLE	The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.
O.AUDIT_GENERATION	The TSF must be able to record defined security-relevant events (which usually include security-critical actions of users of the TOE). The information recorded for security-relevant events must contain the time and date the event happened and, if possible, the identification of the user that caused the event, and must be in sufficient detail to help the authorized user detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.
O.DISCRETIONARY_ACCESS	The TSF must control access of subjects and/or users to named resources based on identity of the object, subject, or user. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.
O.I&A	The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.
O.MANAGE	The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.
O.MEDIATE	The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.
O.RESIDUAL_INFORMATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.
O.TOE_ACCESS	The TOE will provide functionality that controls a user's logical access[2] to user data and to the TSF.

[2] Here, "logical access" is specified, since the control of "physical access" is outside the scope of this PP.

5.2 Operational Environment Security Objectives

Table 5: Operational Environment Security Objectives

Objective 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.INFO_PROTECT	Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.
OE.NO_GENERAL_ PURPOSE	There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration, and support of the DBMS.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.

Table 6: Operational Environment IT Security Objectives

Objective Name	Definition
OE.IT_I&A	Any information provided by a trusted entity in the environment and used to support user authentication and authorization used by the TOE is correct and up to date.
OE.IT_REMOTE	If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions, required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.
OE.IT_TRUSTED_SYSTEM	The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.

6 Extended Security Functional Requirements

FTA_TAH_(EXT).1 TOE access information

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: FTA_TAH_(EXT).1

There are no management activities foreseen.

Audit: FTA_TAH_(EXT).1

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.

FIA_USB_(EXT).2 Enhanced user-subject binding

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 leveling

FIA_USB_(EXT).2 is hierarchical to FIA_USB.1.

Management

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

Audit

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

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].

7 SECURITY REQUIREMENTS

7.1 Security Functional Requirements

This section defines the functional requirements for the TOE. Functional requirements in this PP were drawn directly from Part 2 of the CC [1b], or were based on Part 2 of the CC, including the use of extended components. These requirements are relevant to supporting the secure operation of the TOE.

Table 7: Security Functional Requirements

Functional Components	
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SEL.1	Selective audit
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_RIP.1	Subset residual information protection
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FIA_USB_(EXT).2	Enhanced user subject binding
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_REV.1(1)	Revocation (user attributes)
FMT_REV.1(2)	Revocation (subject, object attributes)
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_TRC.1	Internal TSF consistency
FTA_MCS.1	Basic limitation on multiple concurrent sessions
FTA_TAH_(EXT).1	TOE access history

Functional Components	
FTA_TSE.1	TOE session establishment

7.1.1 Security Audit (FAU)

7.1.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1

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

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

b) All auditable events for the *minimum* level of audit **listed in Table 8: Auditable Events;** and

c) [Start-up and shutdown of the DBMS;

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

e) [selection: [assignment: events at a minimal level of audit introduced by the inclusion of additional SFRs determined by the ST author], [assignment: events commensurate with a minimal level of audit introduced by the inclusion of extended requirements determined by the ST author], "no additional events"]].

Application Note: For the selection, the ST author should choose one or both of the assignments (as detailed in the following paragraphs), or select "no additional events".

Application Note: For the first assignment, the ST author augments the table (or lists explicitly) the audit events associated with the minimal level of audit for any SFRs that the ST author includes that are not included in this PP.

Application Note: Likewise, if the ST author includes extended requirements not contained in this PP, the corresponding audit events must be added in the second assignment. Because "minimal" audit is not defined for such requirements, the ST author will need to determine a set of events that are commensurate with the type of information that is captured at the minimal level for similar requirements.

Application Note: If no additional (CC or extended) SFRs are included, or if additional SFRs are included that do not have "minimal" audit associated with them then it is acceptable to assign "no additional events" in this item.

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 PP/ST, [information specified in

column three of Table 8: Auditable Events, below].

Application Note: 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 8: 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
FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP	The identity of the subject performing the operation
FDP_RIP.1	None	None
FIA_ATD.1	None	None
FIA_UAU.1	Unsuccessful use of the authentication mechanism	None
FIA_UID.1	Unsuccessful use of the user identification mechanism, including the user identity provided	None
FIA_USB_(EXT).2	Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject)	None
FMT_MOF.1	None	None
FMT_MSA.1	None	None
FMT_MSA.3	None	None
FMT_MTD.1	None	None

Column 1: **Security Functional Requirement**	**Column 2** **Auditable Event(s)**	**Column 3** **Additional Audit Record Contents**
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_TAH_(EXT).1	None	None
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism	Identity of the individual attempting to establish a session

7.1.1.2 FAU_GEN.2 User identity association

FAU_GEN.2.1

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

7.1.1.3 FAU_SEL.1 Selective audit

FAU_SEL.1.1

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

a) object identity;

b) user identity;

c) [selection: "subject identity", "host identity "**, "group identity",** "**no other identities**",];

d) event type;

e) [success of auditable security events;

f) failure of auditable security events; and

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

Application Note: "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: The intent of this requirement is to capture enough audit data to allow the administrators to perform their task, not necessarily to capture only the needed audit data. In other words, the DBMS does not necessarily need to include or exclude auditable events based on all attributes at any given time.

7.1.2 User data protection (FDP)

7.1.2.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1

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

7.1.2.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1

The TSF shall enforce the [Discretionary Access Control policy] to objects 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: 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.

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 authorise 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 authorise access of subjects to objects].

7.1.2.3 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1

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

[assignment: list of objects].

7.1.3 Identification and authentication (FIA)

Application Note: 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 I&A services are performed either by the TOE itself or that they are performed within the TOE environment.

7.1.3.1 FIA_ATD.1 User attribute definition

FIA_ATD.1.1

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

a) [Database user identifier and any associated group memberships;

b) Security-relevant database roles; and

c) [assignment: list of security attributes]].

Application Note: 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.

7.1.3.2 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1

The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

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

7.1.3.3 FIA_UID.1 Timing of identification

FIA_UID.1.1

The TSF shall allow [assignment: list of TSF-mediated actions] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

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

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

FIA_USB_(EXT).2 .1

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

7.1.4 Security management (FMT)

7.1.4.1 FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1

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

7.1.4.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1

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

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

7.1.4.3 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1

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

Application Note: This requirement applies to new container 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.

7.1.4.4 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1

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

7.1.4.5 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].

7.1.4.6 FMT_REV.1(2) Revocation

FMT_REV.1.1(2)

The TSF shall restrict the ability to revoke [assignment*:* list of security attributes] associated with the *object*s 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].

7.1.4.7 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: [assignment: list of security management functions to be provided by the TSF].

7.1.4.8 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: This requirement identifies a minimum set of management roles. A ST or 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 writer may change the names of the roles identified above but the "new" roles must still perform the functions that the FMT requirements in this PP have defined.

7.1.5 Protection of the TOE Security Functions (FPT)

Application Note: The security domain boundary in the first element is TSF domain and its intent is to protect the TSF from untrusted subjects at the TSFIs. The security domain boundary in the second element covers the complete TOE Scope of Control and its intent is to maintain separation between any subjects within the TOE Scope of Control.

7.1.5.1 FPT_TRC.1 Internal TSF consistency

FPT_TRC.1.1

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

FPT_TRC.1.2

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

Application Note: This requirement is trivially met if the TOE does not contain physically separated components. Application Note: 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.

7.1.6 TOE Access (FTA)

7.1.6.1 FTA_MCS.1 Basic limitation on multiple concurrent sessions

FTA_MCS.1.1

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

FTA_MCS.1.2

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

Application Note: The ST author is reminded that the CC [REF 1b] para 473 allows that the default number may be defined as a management function in FMT.

7.1.6.2 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.

7.1.6.3 FTA_TSE.1 TOE session establishment

FTA_TSE.1.1

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

7.2 Security Assurance Requirements

All of the assurance requirements included in Evaluation Assurance Level (EAL) 2 augmented with the following additions:

- ALC_FLR.2: Flaw remediation

The following is a list of the assurance requirements needed for this protection profile:

Table 9: Assurance Requirements

Assurance Class	Assurance Components	Assurance Components Description
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life Cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification

8 RATIONALE

This section provides the rationale for the selection of the IT security requirements, objectives, assumptions, and threats. In particular, it shows that the IT security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

8.1 Rationale for TOE Security Objectives

The following tables provide a mapping of security objectives to the environment defined by the threats, policies and assumptions, illustrating that each security objective covers at least one threat, assumption or policy and that each threat, assumption or policy is covered by at least one security objective.

8.1.1 TOE Security Objectives Coverage

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

Table 10: Coverage of Security Objectives for the TOE

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

8.1.2 Rationale for TOE Security Objectives

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

Table 11: 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 will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.	O.ADMIN_ROLE supports this policy by ensuring that the TOE has an objective to provide authorized administrators with the privileges needed for secure administration.
	O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security relevant events associated with users.	O.AUDIT_GENERATION supports this policy by ensuring that audit records are generated. Having these records available enables accountability.
	O.I&A The TOE ensures 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.TOE_ACCESS The TOE will 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 access to authorized users.

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.	O.MANAGE The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.	O.MANAGE supports this policy by ensuring that the functions and facilities supporting the authorized administrator role are in place.
	O.TOE_ACCESS The TOE will 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 access to authorized users.
	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 this policy by ensuring that the authorized administrator role is understood and used by competent administrators.

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 supporting only the administrative duties the person has. This role shall be separate and distinct from other authorized users.	O.ADMIN_ROLE The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.	O.ADMIN_ROLE The TOE has the objective of providing an authorized administrator role for secure administration. The TOE may provide other roles as well, but only the role of authorized administrator is required.
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS supports this policy by ensuring that an authorized administrator role can be distinguished from other authorized users.

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
T.ACCESS_TSFDATA A threat agent may read or modify TSF data using functions of the TOE without the proper authorization.	O.ACCESS_HISTORY The TOE will store information related to previous attempts to establish a session and make that information available to the user.	O.ACCESS_HISTORY diminishes this threat because it ensures the TOE will store the information that is needed to advise the user of previous authentication attempts and allows this information to be retrieved.
	O.I&A The TOE ensures 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 must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.	O.MANAGE diminishes this threat since it ensures that functions and facilities used to modify TSF data are not available to unauthorized users.
	O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.	O.RESIDUAL_INFORMATION diminishes this threat since information contained in protected resources will not be easily available to the threat agent through reallocation attacks.
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS diminishes this threat since it makes it more unlikely that a threat agent has access to the TOE.

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
T.ACCESS_TSFFUNC A threat agent may use or manage TSF, bypassing the protection mechanisms of the TSF.	O.ADMIN_ROLE The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.	O.ADMIN_ROLE diminishes this threat by providing isolation of privileged actions.
	O.I&A The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.	O.I&A diminishes this threat since the TOE requires successful authentication to the TOE prior to gaining access to any controlled-access content. By implementing strong authentication to gain access to these services, an attacker's opportunity to masquerade as another entity in order to gain unauthorized access to data or TOE resources is reduced.
	O.MANAGE The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.	O.MANAGE diminishes this threat because an access control policy is specified to control access to TSF data. This objective is used to dictate who is able to view and modify TSF data, as well as the behavior of TSF functions.
	O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.	O.RESIDUAL_INFORMATION diminishes this threat by ensuring that TSF data and user data is not persistent when resources are released by one user/process and allocated to another user/process.
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS diminishes this threat since it makes it more unlikely that a threat agent has access to the TOE.

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
T.IA_MASQUERADE A user or a process acting on behalf of a user may masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources	O.ACCESS_HISTORY The TOE will store information related to previous attempts to establish a session and make that information available to the user.	O.ACCESS_HISTORY diminishes this threat because it ensures the TOE will be able to store and retrieve the information that will advise the user of the last successful login attempt and performed actions without their knowledge.
	O.I&A The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.	O.I&A diminishes this threat by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE has defined to provide to authenticated users only
	O.MEDIATE The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.	O.MEDIATE diminishes this threat by ensuring that all access to user data are subject to mediation, unless said data has been specifically identified as public data. The TOE requires successful authentication to the TOE prior to gaining access to any controlled-access content. By implementing strong authentication to gain access to these services, an attacker's opportunity to masquerade as another entity in order to gain unauthorized access to data or TOE resources is reduced.
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS diminishes this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanism this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE.

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
T.IA_USER A threat agent may gain access to user data, TSF data or TOE resources with the exception of public objects without being identified and authenticated.	O.DISCRETIONARY_ACCESS The TSF must control access of subjects and/or users to named resources based on identity of the object, subject, or user. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.	O.DISCRETIONARY_ACCESS diminishes this threat by requiring that data including user data stored with the TOE, have discretionary access control protection.
	O.I&A The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.	O.I&A diminishes this threat 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.MEDIATE The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.	O.MEDIATE diminishes this threat by ensuring that all access to user data are subject to mediation, unless said data has been specifically identified as public data. The TOE requires successful authentication to the TOE prior to gaining access to any controlled-access content. By implementing strong authentication to gain access to these services, an attacker's opportunity to masquerade as another entity in order to gain unauthorized access to data or TOE resources is reduced.
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS diminishes this threat by controlling logical access to user data, TSF data or TOE resources.

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 will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.	O.RESIDUAL_INFORMATION diminishes this threat because even if the security mechanisms do not allow a user to view TSF data, if TSF data were to reside inappropriately in a resource that was made available to a user, that user would be able to view the TSF data without authorization.

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
T.TSF_COMPROMISE A user or a process acting on behalf of a use may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable code within the TSF.	O.ACCESS_HISTORY The TOE will store information related to previous attempts to establish a session and make that information available to the user.	O.ACCESS_HISTORY diminishes this threat because it ensures the TOE will be able to store and retrieve the information that will advise the user of the last successful login attempt and performed actions without their knowledge.
	O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security relevant events associated with users.	O.AUDIT_GENERATION diminishes this threat by providing the authorized administrator with the appropriate audit records supporting the detection of compromise of the TSF.
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS diminishes this threat since controlled user's logical access to the TOE will reduce the opportunities for an attacker’s access to configuration data.

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
T.UNAUTHORIZED_ACCESS A user may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.	O.DISCRETIONARY_ACCESS The TSF must control access of subjects and/or users to named resources based on identity of the object, subject or user. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.	O.DISCRETIONARY_ACCESS diminishes this threat by requiring that data including TSF data stored with the TOE, have discretionary access control protection.
	O.MANAGE The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.	O.MANAGE diminishes this threat by ensuring that the functions and facilities supporting that authorized users can be held accountable for their actions by authorized administrators are in place.
	O.MEDIATE The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.	O.MEDIATE diminishes this threat because it ensures that all access to user data are subject to mediation, unless said data has been specifically identified as public data. The TOE requires successful authentication to the TOE prior to gaining access to any controlled-access content. By implementing strong authentication to gain access to these services, an attacker's opportunity to conduct a man-in-the-middle and/or password guessing attack successfully is greatly reduced. Lastly, the TSF will ensure that all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services. The TOE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc. to the administrator. This feature ensures that no other user can modify the information flow policy to bypass the intended TOE security policy.

8.2 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 12: Coverage of SPF Items for the TOE Environment Security Objectives

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

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

Table 13: 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 at least some of the information managed by the TOE.	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. •Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT supports the assumption by ensuring that users are authorized to access parts of the data managed by the TOE and is trained to exercise control over their own data. Having trained, authorized users, who are provided with relevant procedures for information protection supports the assumption of co-operation.
	OE.IT_REMOTE If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions, required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.	OE.IT_REMOTE supports this assumption by ensuring that remote systems that form part of the IT environment are protected. This gives confidence that the environment is benign.
	OE.IT_TRUSTED_SYSTEM The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.	OE.IT_TRUSTED_SYSTEM supports this assumption by providing confidence that systems in the TOE IT environment contribute to a benign environment.

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 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.IT_REMOTE If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions, required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.	OE.IT_REMOTE supports the assumption by levying a requirement in the environment that connections between trusted systems or physically separated parts of the TOE 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 manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and 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
	OE.IT_TRUSTED_SYSTEM The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.	OE.IT_TRUSTED_SYSTEM supports the assumption by ensuring that remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy.

Assumption	Environmental Objective Addressing the Assumption	Rationale for Specifying the Environmental Security Objective
	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.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.

Assumption	Environmental Objective Addressing the Assumption	Rationale for Specifying the Environmental Security Objective
A.MANAGE The TOE security functionality is managed by one or more competent 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 since the authorized administrators are assumed competent in order to help ensure that all the tasks and responsibilities are performed effectively.
	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and 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 the information protection aspects of the TOE and the system(s) and relevant connectivity that form the platform for the TOE is vital to addressing the security problem, described in this PP. Managing these effectively using defined procedures is reliant on having competent administrators.

Assumption	Environmental Objective Addressing the Assumption	Rationale for Specifying the Environmental Security Objective

Assumption	Environmental Objective Addressing the Assumption	Rationale for Specifying the Environmental Security Objective
A.NO_GENERAL_PURPOSE There are no general-purpose computing or storage repository 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 will 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 or storage capabilities. This will protect the TSF data from malicious processes. The environmental objective is tightly related to the assumption, which when fulfilled will address the assumption.

Assumption	Environmental Objective Addressing the Assumption	Rationale for Specifying the Environmental Security Objective
A.PEER_FUNC_&_MGT All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.	OE.IT_REMOTE If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions, required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.	OE.IT_REMOTE The assumption that connections between trusted systems or physically separated parts of the TOE is addressed by the objective specifying that such systems are sufficiently protected from any attack that may cause those functions to provide false results.
	OE.IT_TRUSTED_SYSTEM The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.	OE.IT_TRUSTED_SYSTEM The assumption on all remote trusted IT systems to implement correctly the functionality used by the TSF consistent with the assumptions defined for this functionality is supported by physical and logical protections and the application of trusted policies commensurate with those applied to the TOE.

Assumption	Environmental Objective Addressing the Assumption	Rationale for specifying the Environmental Security Objective
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.	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.PHYSICAL The TOE, the TSF data, and protected user data is assumed to be protected from physical attack (e.g., theft, modification, destruction, or eavesdropping). Physical attack could include unauthorized intruders into the TOE environment, but it does not include physical destructive actions that might be taken by an individual that is authorized to access the TOE environment.
	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and 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 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.	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and 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 is trained to exercise control over their own data.

Policy	Environmental Objective Addressing the Policy	Rationale for Specifying the Environmental Security Objective
P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE.	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 that the authorized administrators are assumed competent in order to help ensure that all the tasks and responsibilities are performed effectively.
	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. •Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT supports the policy by ensuring that the authorized users are trained and have procedures available to support them and that the DAC protections function and are able to provide sufficient information to inform those pursuing accountability.

Policy	Environmental Objective Addressing the Policy	Rationale for Specifying the Environmental Security Objective
P.ROLES The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.	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 an authorized administrator role for secure administration of the TOE is established.

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

Threat	Environmental Objective Addressing the Threat	Rationale for Specifying the Environmental Security Objective
T.IA_MASQUERADE A user or a process acting on behalf of a user may masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources	OE.NO_GENERAL_PURPOSE There will 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 or storage capabilities. This diminishes the threat of masquerade since only users with DBMS or related functions will be defined in the TOE environment.

Threat	Environmental Objective Addressing the Threat	Rationale for Specifying the Environmental Security Objective
T.TSF_COMPROMISE A user or a process acting on behalf of a use may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable code within the TSF.	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT diminishes the threat by ensuring 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_REMOTE If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions, required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.	OE.IT_REMOTE diminishes the threat by ensuring that remote trusted IT systems are sufficiently protected.
	OE.IT_TRUSTED_SYSTEM The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.	OE.IT_TRUSTED_SYSTEM diminishes the threat by ensuring that remote trusted IT systems are managed according to known, accepted and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.
	OE.NO_GENERAL_PURPOSE There will 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 diminishes this threat by reducing the opportunities to subvert non TOE related capabilities in the TOE environment.

Threat	Environmental Objective Addressing the Threat	Rationale for Specifying the Environmental Security Objective
	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.PHYSICAL diminishes the threat of a TSF compromise due to exploitation of physical weaknesses or vulnerabilities as a vector in an attack.

Threat	Environmental Objective Addressing the Threat	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 must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT diminishes the threat by ensuring that the logical and physical threats to network and peripheral cabling are appropriately protected. DAC protections if implemented correctly may support the identification of unauthorized accesses.

8.3 Rationale for Security Functional Requirements

8.3.1 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 14: Rationale for Extended Security Functional Requirements

Extended Requirement	Identifier	Rationale
FTA_TAH_(EXT).1	TOE Access History	This PP does not require the TOE to contain a client. Therefore, the PP cannot require the client to display a message. This requirement has been modified to require the TOE to store and retrieve the access history instead of displaying it.
FIA_USB_(EXT).2	Enhanced user-subject binding	A DBMS may derive subject security attributes from other TSF data that are not directly user security attributes. An example is the point-of-entry the user has used to establish the connection. An access control policy may also use this subject security attribute within its access control policy, allowing access to critical objects only when the user has connected through specific ports-of-entry.

8.3.2 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 15: Rationale for TOE Security Functional Requirements

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS_HISTORY The TOE will store information related to previous attempts to establish a session and make that information available to the user.	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. When appropriately displayed, this will allow the user to detect if another user is attempting to access their account. These records should not be deleted until after the user has been notified of their access history. (FTA_TAH_(EXT).1)
O.ADMIN_ROLE The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.	FMT_SMR.1	The TOE will establish, at least, an authorized administrator role. The ST writer may choose to specify more roles. The authorized administrator will be given privileges to perform certain tasks that other users will not be able to perform. These privileges include, but are not limited to, access to audit information and security functions. (FMT_SMR.1)

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT_GENERATION The TOE will 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. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements a ST author adds to this PP. FAU_GEN.2 ensures that the audit records associate a user and any associated group identity with the auditable event. In the case of authorized users, the association is accomplished with the user ID. In the case of authorized groups, the association is accomplished with the group ID. FAU_SEL.1 allows the administrator to configure which auditable events will be recorded in the audit trail. This provides the administrator with the flexibility in recording only those events that are deemed necessary by site policy, thus reducing the amount of resources consumed by the audit mechanism.
O.DISCRETIONARY_ACCESS The TSF must control access of subjects and/or users to named resources based on identity of the object, subject or user. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.	FDP_ACC.1 FDP_ACF.1	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.1]. The rules for the access control policy are defined [FDP_ACF.1].

Objective	Requirements Addressing the Objective	Rationale
O.I&A The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.	FIA_ATD.1 FIA_UAU.1 FIA_UID.1 FIA_USB_(EXT).2	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.1, FIA_UAU.1]. To ensure that the security attributes used to determine access are defined and available to the support authentication decisions. [FIA_ATD.1]. Proper authorization for subjects acting on behalf of users is also ensured [FIA_USB_(EXT).2]. The appropriate strength of the authentication mechanism is ensured.
O.MANAGE The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_REV.1(1) FMT_REV.1(2) FMT_SMF.1 FMT_SMR.1	FMT_MOF.1 requires that the ability to use particular TOE capabilities be restricted to the administrator. FMT_MSA.1 requires that the ability to perform operations on security attributes be restricted to particular roles. FMT_MSA.3 requires that default values used for security attributes are restrictive. FMT_MTD.1 requires that the ability to manipulate TOE content is restricted to administrators. FMT_REV.1 restricts the ability to revoke attributes to the administrator. 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.

Objective	Requirements Addressing the Objective	Rationale
O.MEDIATE The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.	FDP_ACC.1 FDP_ACF.1 FPT_TRC.1	The FDP requirements were chosen to define the policies, the subjects, objects, and operations for how and when mediation takes place in the TOE. FDP_ACC.1 defines the Access Control policy that will be enforced on a list of subjects acting on the behalf of users attempting to gain access to a list of named objects. All the operations between subject and object covered are defined by the TOE's policy. FDP_ACF.1 defines the security attribute used to provide access control to objects based on the TOE's access control policy. FPT_TRC.1 ensures replicated TSF data that specifies attributes for access control must be consistent across distributed components of the TOE. The requirement is to maintain consistency of replicated TSF data.
O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.	FDP_RIP.1	FDP_RIP.1 is used to ensure the contents of resources are not available to subjects other than those explicitly granted access to the data.

Objective	Requirements Addressing the Objective	Rationale
O.TOE_ACCESS The TOE will 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	FDP_ACC.1 requires that each identified access control SFP be in place for a subset of the possible operations on a subset of the objects in the TOE. FDP_ACF.1 allows the TSF to enforce access based upon security attributes and named groups of attributes. Furthermore, the TSF may have the ability to explicitly authorize or deny access to an object based upon security attributes. FIA_ATD.1 defines the security attributes for individual users including the user's identifier and any associated group memberships. Security relevant roles and other identity security attributes. FTA_MCS.1 ensures that users may only have a maximum of a specified number of active sessions open at any given time. FTA_TSE.1 allows the TOE to restrict access to the TOE based on certain criteria.

8.3.3 Rationale for Satisfying All Security Functional Requirement Dependencies

Table 16: Security Functional Requirement Dependencies

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	satisfied by FAU_GEN.1 satisfied by FIA_UID.1
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	satisfied by FAU_GEN.1 satisfied by FMT_MTD.1
FDP_ACC.1	FDP_ACF.1	satisfied by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	satisfied by FDP_ACC.1 satisfied by FMT_MSA.3.
FDP_RIP.1	None	N/A
FIA_ATD.1	None	N/A
FIA_UAU.1	FIA_UID.1	satisfied by FIA_UID.1
FIA_UID.1	None	N/A
FIA_USB_(EXT).2	FIA_ATD.1	satisfied by FIA_ATD.1
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	satisfied by FMT_SMF.1 satisfied by FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	satisfied by FDP_ACC.1. satisfied by FMT_SMF.1 satisfied by FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	satisfied by FMT_MSA.1 satisfied by FMT_SMR.1
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	satisfied by FMT_SMF.1 satisfied by FMT_SMR.1
FMT_REV.1(1)	FMT_SMR.1	satisfied by FMT_SMR.1
FMT_REV.1(2)	FMT_SMR.1	satisfied by FMT_SMR.1

Requirement	Dependency	Satisfied
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	satisfied by FIA_UID.1
FPT_TRC.1	FPT_ITT.1	FPT_ITT.1 is not applicable For a distributed TOE the dependency is satisfied through the assumption on the environment, A.CONNECT , that assures the confidentiality and integrity of the transmitted data
FTA_MCS.1	FIA_UID.1	satisfied by FIA_UID.1
FTA_TAH_(EXT).1	None	N/A
FTA_TSE.1	None	N/A

8.4 Rationale for Satisfying all Security Assurance Requirements

This protection profile is developed for use by commercial DBMS security software developers. Since the PP will be applied to commercial DBMS products that are used internationally the EAL 2 assurance package was selected by the PP writers to meet the maximum level of assurance that is recognized internationally through the Common Criteria Recognition Arrangement (CCRA).

Flaw Remediation is the only requirement not included in any EAL level because it does not add any assurance to the current system, but to subsequent releases. Therefore, the DBMS WG/TC decided to augment EAL2 with ALC_FLR.2 to instruct the vendors on proper flaw remediation techniques.

The dependencies for security assurance requirements are all fulfilled based on the following facts:

- EAL2 is completely self-sufficient with all dependencies being fulfilled with the package of EAL2.

- The security assurance requirement of ALC_FLR.2, which is in addition to EAL2, does not have any dependencies.

8.5 Conclusion

Based on the security objectives and the security objectives rationale, the following conclusion is drawn: if all security objectives are achieved then the security problem as defined in the Security Problem Definition (SPD) is solved: all threats are countered, all Organizational Security Policies (OSPs) are enforced, and all assumptions are upheld.

9 APPENDICES

The following sections are the appendices for this Protection Profile.

Appendix A. REFERENCES

[REF 1] Common Criteria Management Board, Common Criteria for Information Technology Security Evaluation, CCMB-2012-09, Version 3.1, September 2012

[REF 1a] Common Criteria Management Board, Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, CCMB-2012-09-01, Version 3.1, September 2012

[REF 1b] Common Criteria Management Board, Common Criteria for Information Technology Security Evaluation: Part 2: Security functional requirements, CCMB-2012-09-02, Version 3.1, September 2012

[REF 1c] Common Criteria Management Board, Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, CCMB-2012-09-03, Version 3.1, September 2012

[REF 2] Common Criteria Development Board, CC and CEM addenda, CCDB-2014-03-01, Version 1.0, March 2014

Appendix B. GLOSSARY

The terms and definitions from CC part 1 and the following apply. In case of a conflict, the term or definition given in this document prevails.

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[3] and the disclosure and modification of data.[4]

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 TSP. Administrators may possess special privileges that provide capabilities to override portions of the TSP.

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.

Authentication data – Information used to verify 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 TSP, perform an operation.

Availability – Timely[5], reliable access to IT resources.

Compromise – Violation of a security policy.

Confidentiality – A security policy pertaining to the disclosure of data.

Configuration data – data that is used in configuring the TOE .

---

[3] Hardware and software

[4] Stored or communicated

[5] According to a defined metric

Conformant Product – A Target of Evaluation that satisfied all the functional security requirements in Section 7.1and satisfies all the TOE security assurance requirements in section 7.2 of this document.

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.

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.

Enclave – A collection of entities under the control of a single authority and having a homogeneous security policy. They may be logical, or may be based on physical location and proximity.

Entity – A subject, object, user or another IT device, which interacts with TOE objects, data, or resources.

Executable code within the TSF – The software that makes up the TSF which is in a form that can be run by the computer

External IT entity – Any trusted Information Technology (IT) product or system, outside of the TOE, which may, in accordance with the TSP, perform an operation.

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 within the TSC that contains or receives information and upon which subjects perform operations.

Operating Environment – The total environment in which a TOE operates. It includes the physical facility and any physical, procedural, administrative and personnel controls.

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.

Secure State – Condition in which all TOE security policies are enforced.

Security attributes – TSF data associated with subjects, objects, and users that are used for the enforcement of the TSP.

Security level – The combination of a hierarchical classification and a set of non-hierarchical categories that represent the sensitivity of the information.

Sensitive information – Information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something.

Subject – An entity within the TSC 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.

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.

Appendix C. ABBREVIATIONS AND ACRONYMS

CA	Certificate Authority
CC	Common Criteria
CCIMB	Common Criteria Interpretations Management Board
CM	Configuration Management
COTS	Commercial Off The Shelf
DAC	Discretionary Access Control
DBMS	Database Management System
DBMS PP	Database Management System Protection Profile
EAL	Evaluation Assurance Level
I&A	Identification and Authentication
IT	Information Technology
LAN	Local Area network
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Functional Policies
SFR	Security Functional Requirement
SPD	Security Problem Definition
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSE	TOE Security Environment
TSF	TOE Security Functions
TSFI	TSF Interfaces
TSP	TOE Security Policy