Common Criteria

Database Management System Protection Profile *(DBMS PP)*

May 2000
Issue 2.1

Version	Authors, Reviewers	Change Summary
2.1	**Primary Author:** Howard Smith	1. Address comments raied by evaluators/certifier
2.0	**Primary Author:** Howard Smith **Reviewers:** Steve Hill (Logica), Duncan Harris, Rajiv Sinha	1. Updated to use functional packages for authentication 2. Updates for CEM 1.0 Compliance 3. Updates for CC 2.1/ISO 15408 Compliance 4. Renamed to Database Management System Protection Profile (DBMS.PP)
1.0	**Primary Author**: Jeff DeMello	1. Release for 1998 NISSC.
0.6	**Primary Author**: Steve Pannifer (Logica) **Reviewers**: Rae Burns, Steve Hill (Logica)	1. Address comments raised by evaluators
0.5	**Primary Author**: Jeff DeMello **Reviewers**: Rae Burns, Steve Hill (Logica)	1. Incorporated Rae Burns and Steve Hill comments 2. Reformatted FrameMaker book file.
0.4	**Primary Author**: Jeff DeMello **Reviewers**: Rae Burns, Howard Smith	1. Updated to be compliant with CC v2.0 Final. 2. Replaced FAU_STG.4 with FAU_STG.3. 3. Added table for required management events. 4. Updated IT Threat Agents definitions for Outsiders, System Users, and Database Users. 5. Updated O.INSTALL a) to make wording consistent with b)
0.3	**Primary Author**: Jeff DeMello **Reviewers**: Howard Smith, Rae Burns	1. Added new requirements (FAU_STG.4, FIA_AFL.1, FIA_SOS.1, FIA_UAU.2, FPT_RVM.1, FPT_SEP.1, FTA_TSE.1), and updated associated tables. 2. Updated to be compliant with CC v2.0 Semi-Final. 3. Added Cover, Revisions, Table of Contents, References, and Glossary. 4. Removed T.BADMEDIA, renamed T.ABUSE and T.PHYSICAL, O.ACCESS.DATA, O.ACCESS.REUSE. 5. Removed PP Application Notes. 6. Integrated Howard Smith & Rae Burns comments
0.2	**Primary Author**: Howard Smith **Reviewers**: Jeff DeMello, Rae Burns	1. Second Issue
0.1	**Primary Author**: Howard Smith (Logica) **Reviewers**: Rae Burns	1. First Issue

Contents

May 2000

Contents

May 2000

1 Introduction

1.1 Identification of Protection Profile

1	*Title:*	Database Management System Protection Profile (DBMS.PP)
2	*Registration:*	(to be completed by registrar)
3	*Version:*	2.1
4	*Publication Date:*	May 2000
5	*Author(s):*	Howard Smith
6	*Sponsor:*	Oracle Corporation
7	*CC Version:*	[CC], Version 2.1
8	*Keywords:*	Database, Protection Profile, TCSEC C2, ITSEC F-C2/E2, RDBMS, O-RDBMS
9	*Assurance Level:*	EAL3

1.2 Protection Profile Overview

10 This protection profile specifies security requirements for database management systems in organisations where there are requirements for protection of the confidentiality (on a “need to know” basis), integrity and availability of information stored in the database. Typically such organisations may be handling commercial, military or medical data; the unauthorised disclosure, modification or withholding of such information may have a severe impact on the operations of the organisation.

11 This PP identifies:

- a set of *core requirements* which all compliant databases must provide; *and*
- a set of *authentication packages* (of which one or more must be provided by a compliant database).

12 The Core Requirements provide basic database functionality, including allowing users to be granted the discretionary right to disclose the information to which they have legitimate access to other users.

13 The administrators of these systems have the ability to:

- control and monitor the actions of end users to help ensure they do not abuse their rights within the system,
- control resource consumption of individual users, *and*
- account for users actions.

14 The Authentication Packages provide the means to authenticate the user by:

- *OS Authentication* (the user is authenticated by the host OS and identified to the database); *or*

- *Database Authentication* (the user is identified and authenticated by the RDBMS).

15 The approach of splitting Core Requirements and Authentication Packages has been adopted to ease the maintenance of this protection profile. It is intended that future issues of this protection profile may extend the list of authentication packages offered, for example, to include directory based authentication.

16 Security Targets wishing to claim conformance with this protection profile must state which authentication package are being claimed. PP conformance claims shall either state “DBMS in OS Authentication Mode”, “DBMS in Database Authentication Mode” or “DBMS in OS and Database Authentication Modes”.

2 Target of Evaluation (TOE) Description

2.1 Product Type

17 The product type is a "*Database Management System*" (DBMS).

2.2 General Features - Core Requirements

18 Typically a DBMS is used to provide many users with simultaneous access to a database.

19 A DBMS may be configured in many ways:

- a *stand alone system* with a single database user (e.g. a single user PC based application);
- many database users working at *terminals connected to a central machine* (e.g. a traditional terminal - mainframe environment);
- a *network of intelligent workstations communicating with a central server* (a "client - server" architecture); or
- a *network of intelligent client workstations communicating with an application server*, which in turn is communicating with the DMBS (e.g. a Web browser communicating with a Web Server which is building dynamic pages from a DBMS).

20 In each of the above configurations the data itself may reside on one server machine, or be distributed among many independent servers.

21 In general, a DBMS is simply an application (albeit large) layered on an underlying system (host operating system and/or network services and/or custom software) and is usually an embedded IT component in a specific system in a defined operational environment.

22 A DBMS application may consist of one or more executable images and one or more data files. These will be subject to the administration of underlying system rights as for any other underlying system processes and files.

23 A DBMS may extend the security functionality of an underlying system, for example a database could implement a very much more fine grained privilege mechanism than the host operating system.

2.3 Authentication Packages

24 An authentication package provides the mechanism for the database to authenticate the claimed identity of a user. Within this protection profile this may be provided by the following two mechanisms:

- externally by the host operating system (*OS Authentication*). In this authentication scheme the database relies on the host operating system to identify and authenticate a user which then provides the authenticated user identity to the database. The database uses the provided operating system identity to establish a database iden-

tity (which may be different);

- within the database itself (*Database Authentication*). In this authentication scheme the database verifies the claimed user identity by using its own authentication mechanism.

25 At least one of the above authentication services must be provided by a compliant database.

3 Security Environment

26 This section identifies the IT assets protected by the TOE. It also identifies the threats to those IT assets, the organisational security policies supported by the TOE, and the assumptions for secure usage of the TOE.

3.1 IT Assets

27 The IT assets requiring protection consist of the information stored within the DBMS, the confidentiality, integrity or availability of which could be compromised. The IT assets are:

DB Objects Database objects and the data contained within those database objects. DB objects may be aggregations of data contained in other database objects.

DB Control Data Database control data used by the DBMS to organize and protect the database objects.

DB Audit Data Database audit data generated by the DBMS during operation.

3.2 Threats

28 The assumed threats to TOE security, along with the threat agents which might instigate these threats, are specified below. Each threat statement identifies a means by which the TOE and its underlying system might be compromised.

29 These threats will be countered by:

a) technical security measures provided by the TOE, in conjunction with

b) technical security measures provided by an underlying system, and

c) non-technical operational security measures (personnel, procedural and physical measures) in the environment.

3.2.1 Threat Agents

30 The threat agents are:

Outsiders Persons who are not authorised users of the underlying system (operating system and/or network services and/or custom software).

Database Users Persons who are authorised users of the TOE.

System Users Persons who are authorised users of the underlying system. System Users may be:

a) those persons who are not Database Users; *or*

b) those persons who are Database Users.

External Events Interruptions to operations arising from failures of hardware, power supplies, storage media, etc.

3.2.2 Threats countered by the TOE

31 Threat agents can initiate the following types of threats against the DBMS. The fol-

lowing threats are countered by the DBMS.

T.ACCESS *Unauthorised Access to the Database*. An outsider or system user who is not (currently) an authorised database user accesses the DBMS. This threat includes: *Impersonation* - a person, who may or may not be an authorised database user, accesses the DBMS, by impersonating an authorised database user (including an authorised user impersonating a different user who has different - possibly more privileged - access).

T.DATA *Unauthorised Access to Information*. An authorised database user accesses information contained within a DBMS without the permission of the database user who owns or who has responsibility for protecting the data.

32 This threat includes unauthorised access to DBMS information, residual information held in memory or storage resources managed by the TOE, or DB control data.

T.RESOURCE *Excessive Consumption of Resources*. An authenticated database user consumes global database resources, in a way which compromises the ability of other database users to access the DBMS.

33 This represents a threat to the availability of the information held within a DBMS. For example, a database user could perform actions which could consume excessive resources, preventing other database users from legitimately accessing data, resources and services in a timely manner. Such attacks may be malicious, inconsiderate or careless, or the database user may simply be unaware of the potential consequences of his actions. The impact of such attacks on system availability and reliability would be greatly amplified by multiple users acting concurrently.

T.ATTACK *Undetected Attack*. An undetected compromise of the DBMS occurs as a result of an attacker (whether an authorised user of the database or not) attempting to perform actions that the individual is not authorised to perform.

34 This threat is included because, whatever countermeasures are provided to address the other threats, there is still a residual threat of a violation of the security policy occurring by attackers attempting to defeat those countermeasures.

T.ABUSE.USER *Abuse of Privileges*. An undetected compromise of the DBMS occurs as a result of a database user (intentionally or otherwise) performing actions the individual is authorised to perform.

35 This threat is included because, whatever countermeasures are provided to address the other threats, there is still a residual threat of a violation of the security policy occurring, or the database being placed at risk, as a result of actions taken by authorised database users. For example a database user may grant access to a DB object they are responsible for to another database user who is able to use this information to perform a fraudulent action.

36 Note that this threat does not extend to highly trusted database users: see the assumption A.MANAGE below.

3.2.3 Threats countered by the Operating Environment

T.OPERATE *Insecure Operation.* Compromise of the database may occur because of improper configuration, administration, and/or operation of the composite system.

T.CRASH *Abrupt Interruptions.* Abrupt interruptions to the operation of the TOE may cause security related data, such as database control data and audit data, to be lost or corrupted. Such interruptions may arise from human error (see also T.OPERATE) or from failures of software, hardware, power supplies, or storage media.

T.PHYSICAL *Physical Attack.* Security-critical parts of the TOE or the underlying operating system and/or network services may be subjected to physical attack which could compromise security.

3.3 Organisational Security Policies

P.ACCESS Access to DB objects are determined by:

a) the owner of the DB object; *and*

b) the identity of the database subject attempting the access; *and*

c) the DB object access privileges to the DB object held by the database subject; *and*

d) the database administrative privileges of the database subject; *and*

e) the resources allocated to the subject.

37 Note that this policy includes the following:

a) *Ownership* - DB object owners are responsible for their DB objects; and

b) *Discretionary Access Control* - DB object owners may grant other database users access to or control over their DB objects on a discretionary basis.

c) *Resources* - Database users are authorised to use only their allocated resources.

P.ACCOUNT Database users are accountable for:

a) operations on objects as configured by the owner of the object; *and*

b) actions configured by database administrators.

3.4 Assumptions

38 The TOE is dependent upon both technical IT and operational aspects of its environment.

3.4.1 TOE Assumptions

A.TOE.CONFIG The TOE is installed, configured, and managed in accordance with its evaluated configuration.

3.4.2 Underlying System Assumptions

3.4.2.1 *Physical Assumptions*

A.PHYSICAL The processing resources of the TOE and the underlying system are located within controlled access facilities which prevents unauthorised physical access by Outsiders, System users and Database Users.

3.4.2.2 *Configuration Assumptions*

A.SYS.CONFIG The underlying system (operating system and/or secure network services and or custom software) is installed, configured, and managed in accordance with its secure configuration.

A.ACCESS The underlying system is configured such that only the approved group of individuals may obtain access to the system.

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the underlying system and the security of the information it contains who can be trusted not to abuse their privileges.

3.4.2.3 *Connectivity Assumptions*

A.PEER Any other IT components with which the TOE communicates are assumed to be under the same management control and operate under the same security policy.

A.NETWORK When required by the TOE, in a distributed environment the underlying network services are assumed to be based on secure communications protocols which ensure the authenticity of users.

4 Security Objectives

39 This section first describes the IT security objectives of the TOE and the threats and policies they address. Then the requirements on the operational environment needed to support the TOE IT objectives are presented.

4.1 TOE Security Objectives

40 This section defines the IT security objectives that are to be satisfied by the TOE in combination with the IT security environment. Table 1 correlates the TOE security objectives to each of the threats and security policies, showing that each threat is countered by at least one IT security objective, and that each security policy is satisfied by at least one IT security objective. A *YES* indicates that the identified IT security objective is relevant to the identified threat or security policy.

Threat/Policy	O.I&A.TOE	O.ACCESS	O.AUDIT	O.RESOURCE	O.ADMIN.TOE
T.ACCESS	YES	YES		YES	YES
T.DATA	YES	YES			YES
T.RESOURCE	YES	YES		YES	YES
T.ATTACK	YES	YES	YES		YES
T.ABUSE.USER	YES	YES	YES		YES
P.ACCESS		YES		YES	
P.ACCOUNT		YES	YES		

Table 1: Correlation of Threats and Policies to TOE Security Objectives

41 Chapter 6 provides the rationale as to why the identified security objectives are suitable to counter the identified threats.

O.ACCESS The TOE must provide end-users and administrators with the capability of controlling and limiting access, by identified individuals, or grouping of individuals, to the data or resources they own or are responsible for, in accordance with the P.ACCESS security policy. To this end the TOE has the following more specific objectives:

O.ACCESS.OBJECTS The TOE must prevent the unauthorised or undesired disclosure, entry, modification, or destruction of data and database objects, database views, and database control and audit data.

O.ACCESS.CONTROL The TOE must allow database users who own or are responsible for data to control the access to that data by other authorised database users.

O.ACCESS.RESIDUAL The TOE must prevent unauthorised access to residual data remaining in objects and resources following the use of those objects and resources.

O.RESOURCE The TOE must provide the means of controlling the consumption of database resources by authorised users of the TOE.

O.I&A.TOE The TOE, with or without support from the underlying system, must provide the means of identifying and authenticating users of the TOE.

42 Note that this security objective explicitly allows identification and authentication of database users to be performed either by the TOE or by the underlying system.

O.AUDIT The TOE must provide the means of recording security relevant events in sufficient detail to help an administrator of the TOE to:

a) detect attempted security violations, or potential misconfiguration of the TOE security features that would leave the database open to compromise; *and*

b) hold individual database users accountable for any actions they perform that are relevant to the security of the database in accordance with P.ACCOUNT.

O.ADMIN.TOE The TOE, where necessary in conjunction with the underlying system, must provide functions to enable an authorised administrator to effectively manage the TOE and its security functions, ensuring that only authorised administrators can access such functionality.

4.2 Environmental Security Objectives

43 The following IT security objectives are to be satisfied by the environment in which the TOE is used.

O.ADMIN.ENV The TOE, where necessary in conjunction with the underlying system, must provide functions to enable an authorised administrator to effectively manage the TOE and its security functions, ensuring that only authorised administrators can access such functionality.

O.FILES The underlying system must provide access control mechanisms by which all of the DBMS-related files and directories (including executables, run-time libraries, database files, export files, redo log files, control files, trace files, and dump files) may be protected from unauthorised access.

O.I&A.ENV The underlying operating system must provide a means of identifying and authenticating users when required by the TOE to reliably identify authenticated users.

O.SEP The underlying operating system must provide the means to isolate the TOE Security Functions (TSF) and assure that TSF components cannot tampered with. The TSF components are 1) the files used by the DBMS to store the database and 2) the TOE processes managing the database.

44 The following non-IT security objectives are to be satisfied by procedural and other

measures taken within the TOE environment.

O.INSTALL Those responsible for the TOE must ensure that:

a) The TOE is delivered, installed, managed, and operated in accordance with the operational documentation of the TOE, and

b) The underlying system is installed and operated in accordance with its operational documentation. If the system components are certified they should be installed and operated in accordance with the appropriate certification documentation.

O.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE that are critical to the security policy are protected from physical attack.

O.AUDITLOG Administrators of the database must ensure that audit facilities are used and managed effectively. These procedures shall apply to the database audit trail and/or the audit trail for the underlying operating system and/or secure network services. In particular:

a) Appropriate action must be taken to ensure continued audit logging, e.g. by regular archiving of logs before audit trail exhaustion to ensure sufficient free space.

b) Audit logs must be inspected on a regular basis and appropriate action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future.

c) The system clocks must be protected from unauthorised modification (so that the integrity of the audit timestamps is not compromised).

O.RECOVERY Those responsible for the TOE must ensure that procedures and/or mechanisms are in place to ensure that, after system failure or other discontinuity, recovery without protection (i.e. security) compromise is obtained.

O.QUOTA Administrators of the database must ensure that each user of the TOE is configured with appropriate quotas that are:

a) sufficiently permissive to allow the user to perform the operations for which the user has access;

b) sufficiently restrictive that the user cannot abuse the access and thereby monopolise resources.

O.TRUST Those responsible for the TOE must ensure that only highly trusted users have the privilege which allows them to:

a) set or alter the audit trail configuration for the database;

b) alter or delete any audit record in the database audit trail;

c) create any user account or modify any user security attributes;

d) authorise use of administrative privileges.

O.AUTHDATA Those responsible for the TOE must ensure that the authentication data for each user account for the TOE as well as the underlying system is held securely and not disclosed to persons not authorised to use that account. In particular:

a) The media on which the authentication data for the underlying operating system and/or secure network services is stored shall not be physically removable from the underlying platform by unauthorised users;

b) Users shall not disclose their passwords to other individuals;

c) Passwords generated by the system administrator shall be distributed in a secure manner.

O.MEDIA Those responsible for the TOE must ensure that the confidentiality, integrity and availability of data held on storage media is adequately protected. In particular:

a) The on-line and off-line storage media on which database and security related data (such as operating system backups, database backups and transaction logs, and audit trails) must not be physically removable from the underlying platform by unauthorised users.

b) The on-line and off-line storage media must be properly stored and maintained, and routinely checked to ensure the integrity and availability of the security related data.

c) The media on which database-related files (including database files, export files, redo log files, control files, trace files, and dump files) have been stored shall be purged prior to being re-used for any non-database purpose.

45 The following table illustrates how each of the above objectives counters a threat, supports an TOE Security Objective, supports a policy or maps to a secure usage assumption:

Environmental Objective	***Counters* Threat**	***Supports* TOE Objective**	***Supports* Policy**	***Maps to* Secure Usage Assumptions**
O.INSTALL	T.OPERATE			A.TOE.CONFIG, A.SYS.CONFIG, A.MANAGE
O.PHYSICAL	T.PHYSICAL			A.ACCESS, A.PEER, A.PHYSICAL
O.AUDITLOG		O.AUDIT	P.ACCOUNT	A.MANAGE
O.RECOVERY	T.CRASH			A.MANAGE
O.QUOTA		O.RESOURCE		A.MANAGE

Table 2: Mapping of Environmental Security Objectives to Threats, TOE Security Objectives, Policy, and Secure Usage Assumptions

Environmental Objective	*Counters* Threat	*Supports* TOE Objective	*Supports* Policy	*Maps to* Secure Usage Assumptions
O.TRUST			P.ACCESS	A.MANAGE
O.AUTHDATA		O.I&A.TOE	P.ACCESS	A.MANAGE, A.PEER, A.NETWORK
O.MEDIA	T.CRASH			A.MANAGE
O.ADMIN.ENV		O.ADMIN.TOE		A.MANAGE
O.FILES	T.ACCESS		P.ACCESS	A.MANAGE
O.I&A.ENV	T.ACCESS	O.I&A.TOE	P.ACCESS	A.MANAGE
O.SEP	T.ACCESS		P.ACCESS	A.MANAGE

Table 2: Mapping of Environmental Security Objectives to Threats, TOE Security Objectives, Policy, and Secure Usage Assumptions

5 Security Requirements

5.1 TOE IT Security Functional Requirements - Core Requirements

46 Table 3 below lists the functional components included in this PP.

Component	Name
	Class FAU - Security Audit
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
	Class FDP - User Data Protection
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_RIP.2	Full residual information protection
	Class FIA - Identification and Authentication
FIA_ATD.1	User attribute definition
FIA_UID.1	Timing of identification
FIA_USB.1	User-subject binding
	Class FMT - Security Management
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_REV.1	Revocation
FMT_SMR.1	Security roles

Table 3: List of Security Functional Components

Component	Name
	Class FPT - Protection of the TOE Security Functions
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
	Class FRU - Resource Utilisation
FRU_RSA.1	Maximum quotas
	Class FTA - TOE Access
FTA_MCS.1	Basic limitation on multiple concurrent sessions
FTA_TSE.1	TOE Session establishment

Table 3: List of Security Functional Components

47 In the paragraphs below, “completed” operations (DBMS PP specific selections or lists) are displayed in **bold**. “Uncompleted” operations are displayed in *italics*. DBMS refinements to standard Common Criteria requirements are displayed as SMALL CAPS.

5.1.1 Class FAU - Security Audit

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 DATABASE audit functions;

b) All auditable events for the **basic** level of audit, AS IDENTIFIED IN TABLE 4 BELOW; and

c) [assignment: *other specifically defined DATABASE auditable events*].

Component	Event	Additional Data
FAU_GEN.1	None	None
FAU_GEN.2	None	None
FAU_SAR.1	Reading of information from the DATABASE audit records	None
FAU_SAR.3	None	None
FAU_SEL.1	All modifications to the DATABASE audit configuration that occur while the DATABASE audit collection functions are operating	MODIFIED CONFIGURATION ELEMENT

Table 4: Required Auditable Events

Component	Event	Additional Data
FAU_STG.1	None	None
FAU_STG.4	Actions taken due to audit storage failure.	None
FDP_ACC.1	None	None
FDP_ACF.1	All requests to perform an operation on an DATABASE object covered by the SFP	DATABASE OBJECT IDENTIFIER, REQUESTED ACCESS, ADMINISTRATIVE PRIVILEGE USED
FDP_RIP.2	None	None
FIA_ATD.1	None	None
FIA_UID.1	All use of the DATABASE user identification mechanism, including the DATABASE user identity provided	None
FIA_USB.1	Success and failure of binding of DATABASE user security attributes to a DATABASE subject (e.g. success and failure to create a DATABASE subject)	None
FMT_MSA.1	All modifications of the values of DATABASE security attributes	NEW SECURITY ATTRIBUTE VALUE
FMT_MSA.3	Modifications of the default setting of permissive or restrictive DATABASE rules	None
FMT_MSA.3	All modifications of the initial values of DATABASE security attributes	NEW INITIAL VALUE
FMT_MTD.1	All modifications to the values of TSF data	None
FMT_REV.1	All attempts to revoke DATABASE security attributes	SECURITY ATTRIBUTE
FMT_SMR.1	Modifications to the group of DATABASE users that are part of a DATABASE role	USER IDENTITY, AUTHORISED ROLE
FPT_RVM.1	None	None
FPT_SEP.1	None	None
FRU_RSA.1	All attempted uses of the DATABASE resource allocation functions for resources that are under control of the TSF	None
FTA_MCS.1	Rejection of a new DATABASE session based on the limitation of multiple concurrent DATABASE sessions	None

Table 4: Required Auditable Events

Component	Event	Additional Data
FTA_TSE.1	All attempts at establishment of a DATABASE user session	None

Table 4: Required Auditable Events

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

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

b) For each DATABASE audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other DATABASE audit relevant information*].

FAU_GEN.2.1 The TSF shall be able to associate each auditable DATABASE event with the identity of the DATABASE user that caused the event.

FAU_SAR.1.1 The TSF shall provide **authorised DATABASE users** with the capability to read **all database audit information** from the DATABASE audit records.

FAU_SAR.1.2 The TSF shall provide the DATABASE audit records in a manner suitable for the DATABASE user to interpret the information.

FAU_SAR.3.1 The TSF shall provide the ability to perform **searches and sorting** of DATABASE audit data based on DATABASE user identity [assignment: *additional criteria with logical relations*].

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable DATABASE events from the set of audited DATABASE events based on the following attributes:

a) event type;

b) DATABASE subject identity;

c) DATABASE object identity;

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

FAU_STG.1.1 The TSF shall protect the stored DATABASE audit records from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to **prevent** modifications to the DATABASE audit records.

FAU_STG.4.1 The TSF shall prevent auditable events except those taken by the authorised user with special rights and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full.

5.1.2 Class FDP - Security Attribute Based Access Control

FDP_ACC.1.1 The TSF shall enforce the DATABASE OBJECT **access control SFP** on:

a) DATABASE subjects;

b) DATABASE objects;

c) ALL PERMITTED operations ON DATABASE OBJECTS BY A DATABASE SUBJECT covered by the SFP.

FDP_ACF.1.1 The TSF shall enforce the DATABASE OBJECT **access control SFP** to DATABASE objects based on:

a) the identity of the owner of the database object; and

b) the object access privileges to the database object held by the database subject; and

c) the database administrative privileges of the database subject.

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

a) if the user associated with the database subject is the owner of the database object, then the requested access is allowed; or

b) if the database subject has the database object access privilege for the requested access to the database object, then the requested access is allowed; or

c) otherwise access is denied, unless access is explicitly authorised in accordance with the rules specified in FDP_ACF.1.3.

FDP_ACF.1.3 The TSF shall explicitly authorise access of DATABASE subjects to DATABASE objects based on the following additional rules:

a) if the database subject has a database administrative privilege to override the database object access controls for the requested access to the database object, then the requested access is allowed;

b) [assignment: *rules, based on DATABASE security attributes, that explicitly authorise access of DATABASE subjects to DATABASE objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of DATABASE subjects to DATABASE objects based on the FOLLOWING ADDITIONAL RULES: [assignment: *rules, based on DATABASE security attributes, that explicitly deny access of DATABASE subjects to DATABASE objects*].

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

5.1.3 Class FIA - Identification and Authentication

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

a) database user identity,

b) database object access privileges,

c) database administrative privileges,

d) [assignment: *list of security attributes*].

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the DATABASE user to be performed before the DATABASE user is identified.

FIA_UID.1.2 The TSF shall require each DATABASE user to be successfully identified before allowing any other TSF-mediated actions on behalf of that DATABASE user.

FIA_USB.1.1 The TSF shall associate the appropriate DATABASE user security attributes with DATABASE subjects acting on behalf of that DATABASE user.

5.1.4 Class FMT - Security Management

FMT_MSA.1.1 The TSF shall enforce the DATABASE OBJECT **access control SFP** to restrict the ability to **modify** the DATABASE OBJECT security attributes [assignment: *list of DATABASE security attributes*] to [assignment: *the authorised identified DATABASE roles*].

FMT_MSA.3.1 The TSF shall enforce the DATABASE OBJECT **access control SFP** to provide **restrictive** default values for DATABASE OBJECT security attributes that are used to enforce the DATABASE OBJECT ACCESS CONTROL SFP.

FMT_MSA.3.2 The TSF shall allow [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when A DATABASE object or information is created.

FMT_MTD.1.1 The TSF shall, ACCORDING TO TABLE 5, restrict the ability to PERFORM OPERATIONS on **TSF data** to **database administrative users**.

Component	Operation	TSF Data
FAU_GEN.1	-	-
FAU_GEN.2	-	-
FAU_SAR.1	deletion, modification, addition	the group of DATABASE users with read access right to the DATABASE audit records
FAU_SAR.3	-	-
FAU_SEL.1	maintenance of the rights to view/ modify	the DATABASE audit events
FAU_STG.1	-	-

Table 5: Required Management Events

Component	Operation	TSF Data
FAU_STG.4	a) maintenance b) deletion, modification, addition	actions to be taken in case of DATABASE audit storage failure
FDP_ACC.1	-	-
FDP_ACF.1	managing	the attributes used to make explicit access or denial based decisions
FDP_RIP.2	-	-
FIA_ATD.1	-	-
FIA_UID.1	management	the DATABASE user identities
FIA_USB.1	-	-
FMT_MSA.1	manage	the group of DATABASE roles that can interact with the DATABASE security attributes
FMT_MSA.3	manage	a) the group of DATABASE roles that can specify initial values b) the permissive or restrictive setting of default values for a given DATABASE access control SFP
FMT_MSA.3	-	-
FMT_MTD.1	manage	the group of DATABASE roles that can interact with the TSF data
FMT_REV.1	manage	the group of DATABASE roles that can invoke revocation of DATABASE security attributes
FMT_SMR.1	manage	the group of DATABASE users that are part of a DATABASE role
FPT_RVM.1	-	-
FPT_SEP.1	-	-
FRU_RSA.1	specify	maximum limits for a resource for DATABASE groups and/or individual DATABASE users and/or DATABASE subjects by an DATABASE administrator
FTA_MCS.1	manage	the maximum allowed number of concurrent DATABASE user DATABASE sessions by an DATABASE administrator
FTA_TSE.1	-	-

Table 5: Required Management Events

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the **DATABASE users and DATABASE objects** within the TSC to:

a) authorised database administrators for (users and objects);

b) authorised database users (only for the database objects they own or database objects for which they have been granted database object access privileges allowing them to revoke security attributes).

c) [assignment: *the authorised identified roles*].

FMT_REV.1.2 The TSF shall enforce the rules:

a) revocation of database object access privileges shall take effect prior to all subsequent attempts to establish access to that database object;

b) revocation of database administrative privileges shall take effect prior to when the database user begins the next database session;

c) [assignment: *specification of revocation rules*].

FMT_SMR.1.1 The TSF shall maintain the DATABASE roles:

a) database administrative user;

b) database user;

c) [assignment: *the authorised identified DATABASE roles*].

FMT_SMR.1.2 The TSF shall be able to associate DATABASE users with DATABASE roles.

5.1.5 Class FPT - Protection of the TOE Security Functions

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted DATABASE subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of DATABASE subjects in the TSC.

5.1.6 Class FRU - Resource Utilisation

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [assignment: *controlled DATABASE resources*] that **an individual DATABASE user** can use **over a specified period of time**.

5.1.7 Class FTA - TOE Access

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent DATABASE sessions that belong to the same DATABASE user.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of a [assignment: *default number*] DATABASE sessions per DATABASE user.

FTA_TSE.1.1 The TSF shall be able to deny DATABASE session establishment based on [assignment: *attributes*].

5.2 TOE IT Security Requirements - OS Authentication

48 The OS Authentication Package introduces no additional IT Security Requirements on the TOE.

5.3 TOE IT Security Requirements - Database Authentication

49 The following IT Security Requirements apply when the TOE supplies the Database Authentication Package. These requirements apply to all users configured to be authenticated by the database.

50 Table 6 below lists the functional components included in this authentication package:

Component	Name
	Class FAU - Security Audit
FAU_GEN.1	Audit data generation (Iterated - Additional Audit Events)
	Class FIA - Identification and Authentication
FIA_AFL.1	Authentication failure handling
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication
	Class FMT - Security Management
FMT_MTD.1	Management of TSF data (Iterated - Additional Management Operations)

Table 6: Security Functional Components For Database Authentication Package

5.3.1 Class FAU - Security Audit

FAU_GEN.1.1.2 The TSF shall be able to generate an audit record of the following auditable events:

a) All auditable events for the **basic** level of audit, AS IDENTIFIED IN TABLE 7 BELOW.

Component	Event	Additional Data
FIA_AFL.1	The reaching of the threshold for the unsuccessful DATABASE authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).	None
FIA_SOS.1	Rejection or acceptance by the TSF of any tested DATABASE secret	None
FIA_UAU.1	All use of the DATABASE authentication mechanism	None

Table 7: Required Auditable Events - Database Authentication

5.3.2 Class FIA - Identification and Authentication

FIA_AFL.1.1 The TSF shall detect when [assignment: *number*] unsuccessful DATABASE authentication attempts occur related to [assignment: *list of DATABASE authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful DATABASE authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that DATABASE secrets (PASSWORDS) meet [assignment: *a defined quality metric*].

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the DATABASE user to be performed before the DATABASE user is authenticated.

FIA_UAU.1.2 The TSF shall require each DATABASE user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that DATABASE user.

5.3.3 Class FMT - Security Management

FMT_MTD.1.1.2 The TSF shall, ACCORDING TO TABLE 8, restrict the ability to PERFORM OPERATIONS on DATABASE AUTHENTICATION RELEVANT TSF DATA to **database administrative users**.

Component	Operation	TSF Data
FIA_AFL.1	management	a) the threshold for unsuccessful DATABASE authentication attempts b) actions to be taken in the event of an DATABASE authentication failure
FIA_SOS.1	management	the metric used to verify the DATABASE secrets
FIA_UAU.1	management	a) the DATABASE authentication data b) the DATABASE authentication data by the associated DATABASE user c) the action lists, if an authorised DATABASE administrator can change the actions allowed before authentication

Table 8: Required Management Events - Database Authentication

5.4 IT Assurance Requirements

51 The target assurance level is EAL3 as defined in Part 3 of the CC. No augmented assurance requirements are defined.

5.5 Security Requirements for the IT Environment - Core Requirements

52 The underlying operating system and/or network services and/or customer software (collectively the *system*) shall support the security objectives of the TOE as follows:

- **O.I&A.TOE**. The system shall identify and authenticate users prior to providing access to any TOE facilities.
- **O.ACCESS**. The system shall provide the access control mechanisms required to support O.FILES and A.NETWORK. In addition these mechanisms are required to support O.AUTHDATA and O.ADMIN.TOE
- **O.AUDIT & O.AUDITLOG**. The system shall provide an audit mechanism and associated audit management tools to support the TOE, particularly in the case where the system mechanisms are used to authenticate users, or the database audit trail is being written to the system audit trail rather than within the database. To ensure the accuracy of the timestamps in both the database and system audit trails the audit trail the system should support FPT_STM.1.

- **O.RESOURCE**. The system may support this objective by providing it's own resource management facilities, although the TOE mechanisms can be used to fully satisfy this objective.
- **O.RECOVERY**. The system shall provide backup, restore and other secure recovery mechanisms.

53 Security objectives not explicitly referred to above are satisfied entirely by the TOE.

54 It should be noted that the requirements for the IT Environment have not been specified using [CC] part 2 functional components. This is a deliberate decision since the wide variety of devices on which a database might reside (e.g. main frame to hand held or embedded device) makes detailed specification impractical.

55 In addition to the above the system shall provide mechanisms to ensure that the system security functions are always invoked prior to passing control to the TOE and that non TOE activity within the system does not interfere with the operation of the TOE. Thus the system shall at least support FPT_RVM.1 and FPT_SEP.1. Also the underlying platform should perform testing to demonstrate the security assumptions made about the underlying abstract machine upon which the TSF relies. Therefore the system shall also support FPT_AMT.

56 It is intended that the above requirements should be satisfied by a system meeting the functional and assurance requirements as defined in the [TCSEC] Class C2 requirements, [ITSEC] Class F-C2/E3 requirements, equivalent [CC] protection profiles (e.g. [CAPP]), or equivalent.

5.6 Security Requirements for the IT Environment - OS Authentication

57 The underlying operating system and/or network services and/or customer software (collectively the *system*) shall support the security objectives of the TOE for users where OS Authentication is configured as follows:

- **O.I&A.TOE**. The system shall identify and authenticate users prior to providing access to any TOE facilities. It is expected that the underlying OS would provide FIA_AFL.1, FIA_SOS.1 and FIA_UAU.1 or equivalent functionality in order to provide the TOE with an authenticated identity.

5.7 Security Requirements for the IT Environment - Database Authentication

58 No additional IT Environment Requirements are specified.

5.8 Minimum Strength of Function

59 The minimum strength of function for this Protection Profile is *SOF-Medium.*

6 Rationale

6.1 Security Objectives Rationale

60 This section provides a demonstration of why the identified security objectives (Paragraph 4) are suitable to counter the identified threats and meet the stated security policies (Paragraph 3.3), as stated in Table 1. The rationale for environmental security objectives is provided by Table 2.

6.1.1 T.ACCESS Rationale

61 T.ACCESS (*Unauthorised Access to the Database)* is directly countered by O.I&A.TOE which ensures the TOE can protect the global data and resources of the database from access by persons not authorised to use that database. O.I&A.TOE ensures the TOE, in conjunction with the underlying operating system, has the means of authenticating the claimed identity of any user. O.ACCESS.CONTROL, O.ADMIN.TOE and O.RESOURCE provide support by controlling access to database control data and administrative functionality that might otherwise enable circumvention of database access controls. O.SEP, O.FILES and O.I&A.ENV together prevent bypass of the TOE.

6.1.2 T.DATA Rationale

62 T.DATA (*Unauthorised Access to Information)* is directly countered by O.ACCESS.OBJECTS. O.ACCESS.OBJECTS ensures access is controlled to information contained within specific database objects. O.ACCESS.RESIDUAL ensures access is prevented to residual information held in memory or reused database objects. O.I&A.TOE provides support by providing the means of identifying the user attempting to access a database object. O.ACCESS.CONTROL and O.ADMIN.TOE provide support by controlling access to database control data and administrative functionality that might otherwise enable circumvention of database object access controls.

6.1.3 T.RESOURCE Rationale

63 T.RESOURCE (*Excessive Consumption of Resources)* is countered directly by O.RESOURCE, which ensures the TOE has the means of limiting the consumption of such resources, including the enforcement of limits on the number of concurrent sessions an individual may have. O.I&A.TOE provides support by providing the means of identifying the user attempting to use resources. O.ACCESS.CONTROL and O.ADMIN.TOE provide support by controlling access to database control data and administrative functionality that might otherwise enable circumvention of resource utilisation controls.

6.1.4 T.ATTACK Rationale

64 T.ATTACK (*Undetected Attack)* is countered directly by O.AUDIT, which ensures the TOE has the means of recording security relevant events which could be indicative of an attack aimed at defeating the TOE security features. O.I&A.TOE provides support

by reliably identifying the user responsible for particular events, where the attacker is an authorised user of the database. O.ACCESS.CONTROL and O.ADMIN.TOE provide support by controlling access to audit configuration data which only highly trusted individuals must be allowed to view and modify.

6.1.5 T.ABUSE.USER Rationale

65 T.ABUSE.USER (*Abuse of Privilege)* is countered directly by O.AUDIT, which ensures the TOE has the means of recording security relevant events which could be indicative of abuse of privilege by an authorised user of the database (whether intentional or otherwise). O.I&A.TOE provides support by reliably identifying the user responsible for particular events, thus ensuring that the user can be held accountable for actions for which he or she is responsible. O.ACCESS.CONTROL and O.ADMIN.TOE provide support by controlling access to audit configuration data which only highly trusted individuals must be allowed to view and modify.

6.1.6 T.OPERATE

66 T.OPERATE is directly provided by O.INSTALL, which ensures that the TOE and its underlying platform are correctly installed, managed and operated.

6.1.7 T.PHYSICAL

67 T.PHYSICAL is directly provided by O.PHYSICAL, which protects critical parts of the TOE from physical attack.

6.1.8 T.CRASH

68 T.CRASH is satisfied by O.MEDIA and O.RECOVERY. These ensure that suitable recovery mechanisms are in place to recover from a crash and that the media used during the crash recovery is able to maintain the confidentially, integrity and availability of the TOE.

6.1.9 P.ACCESS Rationale

69 P.ACCESS is satisfied by O.ACCESS.OBJECTS and O.RESOURCE. O.ACCESS.OBJECTS ensures that the subjects using the TOE are able to control access to the objects which they own or for which they are responsible. O.RESOURCE ensures that the TOE is able to control the consumption of resources.

6.1.10 P.ACCOUNT Rationale

70 P.ACCOUNT is directly satisfied by O.AUDIT which ensures that the subjects using the TOE are accountable for their actions by recording details of attempted security violations and other actions which have been configured for auditing. P.ACCOUNT is also indirectly satisfied by O.ACCESS which ensures that the accounting data is protected.

6.2 Security Requirements Rationale - Core Services

6.2.1 Suitability of Security Requirements

71 Table 9 correlates the IT security objectives to the SFRs which satisfy them (as indicated by a *YES*), showing that each IT security objective is satisfied by at least one SFR, and that each SFR satisfies at least one IT security objective.

Requirement	O.I&A.TOE	O.ACCESS	O.AUDIT	O.RESOURCE	O.ADMIN.TOE
FAU_GEN.1			YES		
FAU_GEN.2			YES		
FAU_SAR.1			YES		
FAU_SAR.3			YES		
FAU_SEL.1			YES		
FAU_STG.1			YES		
FAU_STG.4			YES		
FDP_ACC.1		YES			
FDP_ACF.1		YES			
FDP_RIP.2		YES			
FIA_ATD.1	YES	YES	YES	YES	YES
FIA_UID.1	YES	YES			
FIA_USB.1	YES	YES	YES	YES	YES
FMT_MSA.1	YES	YES			YES
FMT_MSA.3		YES			
FMT_MTD.1	YES		YES	YES	YES
FMT_REV.1		YES			
FMT_SMR.1					YES
FPT_RVM.1		YES			
FPT_SEP.1		YES			
FRU_RSA.1				YES	
FTA_MCS.1	YES			YES	
FTA_TSE.1	YES			YES	

Table 9: Correlation of IT Security Objectives to Security Functional Requirements

6.2.1.1 *O.I&A.TOE Suitability*

72 O.I&A.TOE is directly provided by FIA_UID.1 which provides the means of identifying users of the TOE. FIA_ATD.1 provides a unique set of user attributes for each user while FMT_MSA.1 and FMT_MTD.1 specify controls over the modification of these attributes. FIA_USB.1 provides an association between these user security attributes with subjects acting on behalf of the user. FTA_MCS.1 and FTA_TSE.1 control the ability to create a database session by a user.

6.2.1.2 *O.ACCESS Suitability*

73 O.ACCESS is directly provided by FDP_ACC.1 which defines the access control policy and FDP_ACF.1 which specifies the access control rules. FMT_REV.1 enforces revocation of security attributes. FDP_RIP.2 ensures prevention of access to information residing in reused storage objects when they are re-allocated to another subject. FIA_USB.1, in conjunction with FIA_ATD.1, ensures the security attributes of a user are bound to subjects created to act on his or her behalf. FIA_UID.1 ensures users are identified prior to any TSF-mediated access actions. FPT_RVM.1 ensures that the traditional reference monitor is always invoked prior to access. FMT_MSA.1 and FMT_MSA.3 provide support for the management of security attributes to control access to database objects. FPT_SEP.1 assures that objects one subject are accessing cannot be intentionally or inadvertently accessed by another subject without a TSF access decision being made for the second subject.

6.2.1.3 *O.AUDIT Suitability*

74 O.AUDIT is directly provided by FAU_GEN.1 which generates audit records for all security relevant events. FAU_GEN.2, in conjunction with FIA_USB.1, supports the enforcement of individual accountability by ensuring the user responsible for each event can be identified. FIA_ATD.1 provides for the storage of user security attributes. FAU_STG.1 provides permanent storage for the audit trail, FAU_STG.4 provides for mechanisms to deal with full audit trails, while FMT_MTD.1 provides for protection of that audit trail. FAU_SAR.1 and FAU_SAR.3 provide functions to review the contents of the audit trail, while FAU_SEL.1 provides the ability to select which events are to be audited.

6.2.1.4 *O.RESOURCE Suitability*

75 O.RESOURCE is provided by:

a) FRU_RSA.1, which provides the means of controlling consumption of resources by individual users (supported by FIA_USB.1 in conjunction with FIA_ATD.1); and

b) FTA_MCS.1, which provides the means of controlling the number of multiple concurrent sessions a user may have, while FTA_TSE.1 provides the means to deny session establishment; and

c) FMT_MTD.1 restricts the control of resource assignment to administrative users.

6.2.1.5 *O.ADMIN.TOE Suitability*

76 O.ADMIN.TOE is directly provided by FMT_SMR.1, which provides essential administrative functionality which is restricted to authorised administrators (FMT_MSA.1 and FMT_MTD.1). FIA_USB.1, in conjunction with FIA_ATD.1, provides support by ensuring that the security attributes of users are associated with subjects acting on the user's behalf.

6.2.2 Dependency Analysis

77 Table 10 demonstrates that all dependencies of functional components are satisfied.

Component Reference	Component	Dependencies	Dependency Reference
1	**FAU_GEN.1**	FPT_STM.1	see note a)
2	**FAU_GEN.2**	FAU_GEN.1 FIA_UID.1	1 12
3	**FAU_SAR.1**	FAU_GEN.1	1
4	**FAU_SAR.3**	FAU_SAR.1	3
5	**FAU_SEL.1**	FAU_GEN.1 FMT_MTD.1	1 16
6	**FAU_STG.1**	FAU_GEN.1	1
7	**FAU_STG.4**	FAU_STG.1	6
8	**FDP_ACC.1**	FDP_ACF.1	9
9	**FDP_ACF.1**	FDP_ACC.1 FMT_MSA.3	8 15
10	**FDP_RIP.2**	-	-
11	**FIA_ATD.1**	-	-
12	**FIA_UID.1**	-	-
13	**FIA_USB.1**	FIA_ATD.1	11
14	**FMT_MSA.1**	FDP_ACC.1 FMT_SMR.1	8 18
15	**FMT_MSA.3**	FMT_MSA.1 FMT_SMR.1	14 18
16	**FMT_MTD.1**	FMT_SMR.1	18
17	**FMT_REV.1**	FMT_SMR.1	18

Table 10: Functional Component Dependency Analysis

Component Reference	Component	Dependencies	Dependency Reference
18	**FMT_SMR.1**	FIA_UID.1	12
19	**FPT_RVM.1**	-	-
20	**FPT_SEP.1**	-	-
21	**FRU_RSA.1**	-	-
22	**FTA_MCS.1**	FIA_UID.1	12
23	**FTA_TSE.1**	-	-

Table 10: Functional Component Dependency Analysis

78 The following dependencies are **not** satisfied in this PP because they are not considered relevant to the threat:

a) FPT_STM.1 has not been included since it is considered a matter for the host operating system to provide the *reliability* of the time stamps used for the TSF. The IT environment section includes this requirement.

79 It is asserted that EAL3 constitutes a set of assurance requirements for which component dependencies are known to be satisfied. Hence no detailed dependency analysis is required for such components.

6.2.3 Demonstration of Mutual Support

80 The dependency analysis provided in the preceding section demonstrates mutual support between functional components, showing that all dependencies required by Part 2 of the CC are satisfied.

81 The following additional supportive dependencies exist between the identified SFRs:

a) FIA_UID.1 together with FIA_ATD.1, FMT_MSA.1 and FIA_USB.1 provide support to all SFRs which rely on the identification of individual users and their security attributes, namely: FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_SMR.1, FRU_RSA.1, FTA_MCS.1, FAU_GEN.1., FAU_GEN.2, FMT_MTD.1, FAU_SAR.1 and FAU_SEL.1.

b) FDP_RIP.2 supports FDP_ACC.1 and FDP_ACF.1 by preventing the bypassing of those SFRs through access to reused storage objects.

c) FMT_MSA.3 provides support to FDP_ACC.1 and FDP_ACF.1 by ensuring objects are protected by default when newly created.

d) FMT_MSA.1 provides support to FDP_ACC.1 and FDP_ACF.1 by controlling the modification of object security attributes.

e) FPT_REV.1 provides support to FMT_MSA.1, FDP_ACC.1 and FDP_ACF.1 by enforcing revocation of object security attributes.

f) FAU_STG.1 and FAU_STG.4 supports FAU_GEN.1 by providing permanent storage for the audit trail, and dealing with when the audit trail is full.

g) FMT_MTD.1 supports FAU_STG.1 and FAU_STG.4 by protecting the integrity of the audit trail.

h) FAU_SEL.1 supports FAU_STG.1 by providing the means of limiting the events to be audited, thereby ensuring that the available space for the audit trail is not exhausted more frequently than necessary.

i) FPT_RVM.1 and FPT_SEP.1 supports FDP_ACC.1 and FDP_ACF.1 by restricting access to residual data and providing separate domains.

j) FRU_RSA.1 and FDP_ACF.1 together satisfy the access control policy P.ACCESS. If a user does not have sufficient resource to access an object, the access will be denied although the other aspects of P.ACCESS are fulfilled.

k) FDP.ACC.1 and FDP.ACF.1 support FAU_STG.1 by preventing unauthorised modifications to the audit trail; the also support FMT_MSA.1.1 by preventing unauthorised modifications of database objects security attributes as well as protecting the TSF data from unauthorised modification supporting FMT_MTD.1.

82 By definition, all assurance requirements support all SFRs since they provide confidence in the correct implementation and operation of the SFRs.

6.3 Security Requirements Rationale - OS Authentication

83 OS Authentication requires that the underlying platform provide an authenticated user identity to the database. This has been reflected in the security requirements for the IT Environment (section 5.6).

6.3.0.1 *O.I&A.TOE Suitability*

84 O.I&A.TOE Identification and authentication checks are performed by the underlying operating system, as is protection of the authentication data.

6.4 Security Requirements Rationale - Database Authentication

6.4.1 Suitability of Security Requirements

85 Table 11 correlates the IT security objectives to the SFRs which satisfy them (as indicated by a *YES*), showing that each IT security objective is satisfied by at least one

SFR, and that each SFR satisfies at least one IT security objective.

Requirement	O.I&A.TOE	O.ACCESS	O.AUDIT	O.RESOURCE	O.ADMIN.TOE
FIA_AFL.1	YES				
FIA_SOS.1	YES				
FIA_UAU.1	YES				

Table 11: Correlation of IT Security Objectives to Security Functional Requirements - Database Authentication

6.4.1.1 *O.I&A.TOE Suitability*

86 Additional support for O.I&A.TOE is provided by the addition of Identification and Authentication checks performed by the database. FIA_SOS.1 provides for quality metrics to be applied when new passwords are chosen. FIA_UAU.1 ensures users to be successfully authenticated prior to any TSF-mediated actions. FIA_AFL performs certain actions if a specified number of unsuccessful authentication attempts is succeeded.

6.4.2 Dependency Analysis

87 Table 10 demonstrates that all dependencies of functional components are satisfied.

Component Reference	Component	Dependencies	Dependency Reference
1	**FIA_AFL.1**	FIA_UAU.1	3
2	**FIA_SOS.1**	-	-
3	**FIA_UAU.1**	FIA_UID.1	(see Table 10, 12)

Table 12: Functional Component Dependency Analysis

6.5 Assumptions Rationale

88 Each assumption (section 3.4) maps to one or more security objectives (section 4) as illustrated in Table 2. The rationale is provided as follows:

a) A.TOE.CONFIG is directly provided by O.INSTALL part a);

b) A.SYS.CONFIG is directly provided by O.INSTALL part b);

c) A.PHYSICAL is directly provided by O.PHYSICAL;

d) A.PEER is directly provided by O.PHYSICAL. Since connected systems will require a physical connection to the TOE to be established they fall into the scope of O.PHYSICAL;

e) A.ACCESS is directly provided by O.PHYSICAL;

f) A.NETWORK is directly provided by O.AUTHDATA. Since the network may be used to transport authentication data it clearly falls into scope of O.AUTHDATA;

g) A.MANAGE is provided by O.TRUST, supported by O.INSTALL, O.AUDITLOG, O.QUOTA, O.AUTHDATA, O.MEDIA, O.ADMIN.ENV, O.FILES, O.I&A.ENV, O.SEP.

6.6 Strength of Functions Rationale

89 The DBMS.PP is targetted at a generalised IT environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have a moderate attack potential, as described in Table 13 below:

Threat Agent	Expertise	Resources	Motivation
Outsiders	Low to Moderate	No IT resources are directly available.	Low to Moderate.
Database Users	Moderate	A valid database account from which further attacks could be made on the database. Additional facilities may be available in the client host environment.	Moderate
System Users	Moderate	A valid account in a client host OS (for example), and other IT facilities provided by client. This user would first have to compromise a database account in order to mount an attack on the database.	Moderate
External Events	External events are random in occurance and effect. These are countered by the administration of the TOE and its environment.		

Table 13: Threat Agents and Attack Potential

90 Of the security objectives, only O.I&A.TOE has a strength related component (the authentication mechanism). When OS Authentication is being used this is provided by the host OS, when DBMS Authentication is being used this is provided by the

TOE.

91 A Strength of Functions of *medium* is therefore appropriate for a database operating in the environment envisaged by this protection profile.

92 It is likely however that many products may wish to offer higher Strength of Functions and this will be reflected in the products' Security Target.

6.7 Security Assurance Rationale

93 A target assurance level of EAL 3 is appropriate for a product designed to be used with operating systems also assured to EAL 3. This is consistent with a product targeted at the [TCSEC] C2 level of assurance, which typically mapped to an [ITSEC] E2 assurance level. This is the minimum level of assurance appropriate for such a product. In practice it is expected that some products may seek assurance to higher levels, and this will be reflected in the Security Target.

94 It should be noted that the possibility of tampering and bypass will be addressed as part of the assurance requirements (e.g. vulnerability analysis AVA_VLA). The role of supporting mechanisms provided by the host operating system will be addressed also in ADV_HLD.2.

7 Application Notes

7.1 Intended use of this PP

95 Any TOE claimed to be compliant with this PP must, as a minimum, provide all SFRs as specified in Core Requirements (section 5.1).

96 Additionally, any compliant TOE must identify and provide at least one of the authentication packages identified in sections 5.2 and 5.3. For each claimed Authentication package the TOE must provide all relevant SFRs identified in sections 5.2 or 5.3 in addition to those in section 5.1. In other words the TOE must satisfy all SFRs for the relevant functional package, these are defined in the following sections in terms of:

- the SFRs for the Database Core Requirements that are modified; *and*
- the SFRs that are additional to the SFRs for the database Core Requirements.

7.2 Functional Packages for Authentication Package (OS Authentication)

97 The OS Authentication Package functional package is defined as follows:

Security Objective	The O.I&A.TOE requirement for the IT Environment is strengthened for OS Authentication.
Modified/Iterated SFRs	None
Additional SFRs	None

7.3 Functional Packages for Authentication Package (Database Authentication)

98 The Database Authentication Package functional package is defined as follows:

Security Objective	None.
Modified/Iterated SFRs	FAU_GEN.1, FMT_MTD.1
Additional SFRs	FIA_AFL.1, FIA_SOS.1, FIA_UAU.1

99 An ST author claiming conformance with the database authentication package may repeat (or reference) the iterated components as per this PP, or could amalgamate the relevant tables into a single table in the ST.

ANNEX

A References

[CC] *Common Criteria for Information Technology Security Evaluation*, Version 2.1, ISO/IEC 15408, CCIB-99-031, 032 & 033, August 1999.

[CEM] *Common Methodology for Information Technology Security Evaluation*, Version 1.0, August 1999, CEM-99/045

[ITSEC] *Information Technology Security Evaluation Criteria* Commission of the European Communities Issue 1.2, 28 June 1991

[TCSEC] *Trusted Computer Security Evaluation Criteria* DoD 5200.28-STD Department of Defense United States of America December 1985

[CAPP] *Controlled Access Protection Profile*, Version 1.d, NSA, October 1999

ANNEX

B Glossary

Acronyms

EAL	Evaluation Assurance Level
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of function
TOE	Target Of Evaluation
TSC	TOE Scope of Control
TSFI	TSF Interface
TSP	TOE Security Policy

Terms

Administrative privilege	A privilege authorising a subject to perform operations that may bypass, alter, or indirectly affect the enforcement of the TSP.
Assets	Information or resources to be protected by the TOE. [CC]

Database	A collection of data that is treated as a unit; the general purpose of a database is to store and retrieve related information.
Database administrative user	A database user to whom one or more administrative privileges have been granted.
Database connection	A communication pathway between a user and a DBMS.
Database non-administrative user	A database user who only has privileges to perform operations in accordance with the TSP.
Database object	An object contained within a database.
Database object access privilege	A privilege authorising a subject to access a named database object.
Database session	A connection of an identified and authenticated user to a specific database; the session lasts from the time the user connects (and is identified and authenticated) until the time the user disconnects.
Database subject	A subject that causes database operations to be performed.
Database user	A user who interacts with a DBMS and performs operations on objects stored within the database.
Evaluation Assurance Level (EAL)	A predefined set of assurance components from Part 3 [of the CC] that represents a point on the CC assurance scale. [CC]
Object	An entity within the TSC that contains or receives information and upon which subjects perform operations. Objects are visible through the TSFI and are composed of one or more TOE resources encapsulated with security attributes. [CC]
Owner	The owner of a named database object is the database user who is responsible for the object and may grant other database users access to the object on a discretionary basis.
Privilege	A right to access objects and/or perform operations that can be granted to some users and not to others.
Product	A package of IT software, firmware, and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems. [CC]
Role (CC)	A predefined set of rules establishing the allowed interactions between a user and the TOE. [CC]
Security attribute	Information associated with subjects, users, and/or objects which is used for the enforcement of the TSP. [CC]
Security domain	The set of objects that a subject has the ability to access. [TCSEC]
Security Function (SF)	A part or parts of the TOE which have to be relied upon for enforcing a closely related subset of the rules from the TSP. [CC]

Security Function Policy (SFP)	The security policy enforced by a SF. [CC]
Security Functional Requirement (SFR)	A security functional requirement defined in a protection profile or security target. [CC]
SOF-medium	A level of TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possession a moderate attack potential. [CC]
Strength of function (SOF)	A qualification of a TOD security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms. [CC]
Subject	An entity within the TSC that causes operations to be performed. [CC]
Target Of Evaluation (TOE)	The product or system being evaluated. [CC]
TOE resource	Anything usable or consumable in the TOE. [CC]
TOE Scope of Control (TSC)	The set of interactions which can occur with or within a TOE and are subject to the rules of the TSP. [CC]
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected and distributed within a TOE. [CC]
TSF Interface (TSFI)	A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF. [CC]
User	Any entity (human or machine) outside the TOE that interacts with the TOE. [CC]