Common Criteria

Commercial Database Management System Protection Profile *(C.DBMS PP)*

March 1998
Issue 1.0

Contents

March 1998

Contents

1 Introduction

1.1 Identification of Protection Profile

1 This is the first definitive issue of the Commercial Database Managemen System Protection Profile and is dated 19th March 1998. This version is intended to be compliant with Issue 2.0 of the CC.

1.2 Protection Profile Overview

2 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.

3 This protection profile allows users to be granted the discretionary right to disclose the information to which they have legitimate access to other users.

4 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.

2 Target of Evaluation (TOE) Description

5 Typically a database management system (DBMS) is used to provide many users with simultaneous access to a database.

6 A DBMS may be configured in many ways:

- a stand alone system with a single user (e.g. a single user PC based application);
- many users working at dumb 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).

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

8 In general a DMBS is simply an application (albeit large) as far as the operating system is concerned. 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 operating system rights as for any other operating system processes and files.

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

3 Security Environment

3.1 Threats

3.1.1 IT Assets and Threat Agents

10 The IT assets requiring protection comprise the information stored within the database, the confidentiality, integrity or availability of which could be compromised.

11 The threat agents are:

Outsiders Persons who are not authorised users of the underlying operating system and/or network services (and hence cannot be authorised users of the TOE);

System Users Persons who are authorised users of the underlying operating system and/or network services. System users may be:

a) system users who are not authorised database users; or

b) system users who *are* authorised database users.

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

12 It is intended that all threats arising from outsiders are countered by technical security measures provided by the underlying operating system and/or network services, in conjunction with appropriate non-technical security measures. However, it is necessary to consider threats arising from outsiders in order to show that the TOE can be adequately protected from these threats by the underlying platform.

13 There are two forms of attack that might be carried out:

a) Unauthorised access to objects, resources and services; and

b) Impersonation.

14 The assumed threats to security are specified below. Each threat statement identifies a means by which the IT assets requiring protection might be compromised. These threats will be countered by technical security measures provided by the TOE, in conjunction with technical security measures provided by an underlying secure platform (comprising a secure operating system and/or network services) and appropriate non-technical security measures (personnel, procedural and physical measures) in the environment.

3.1.2 Threats countered by the DBMS and its IT environment

T.ACCESS *Unauthorised Access to the Database.* An outsider or system user who is not (currently) an authorised database user accesses the database.

15 This threat includes:

a) A person, who may or may not be an authorised database user, accesses the database, by impersonating an authorised database user (including an authorised user impersonating a different user who has different - possibly more privileged - access rights); and

b) A person, who may or may not be a database user accesses the database anonymously (for example, accesses a remote database under a user id shared with user users of the link or gains access to the database files via the host operating system and thereby bypasses the DBMS altogether); this also includes passive attacks (e.g. monitoring of network traffic).

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

16 This threat includes unauthorised access to database information, residual information held in memory or storage resources returned to the TOE, or database control data.

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

17 This represents a threat to the availability of the information held within a database.

T.ATTACK *Undetected Attack*. An undetected compromise of the IT assets 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.

18 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 *Abuse of Privilege*. An undetected compromise of the IT assets occurs as a result of an authorised database user (intentionally or otherwise) performing actions the individual is authorised to perform.

19 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 IT assets being placed at risk, as a result of actions taken by authorised users of the database. For example, an authorised database user could perform actions which could consume excessive resources, preventing other authorised database users from legitimately accessing data, resources and services in a timely manner. Such attacks may be malicious, inconsiderate or careless, or the 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.

20 Note that this threat does not extend to highly trusted users: see the threat

T.TRUSTED below.

3.1.3 Threats countered by the Operating Environment

T.OPERATE *Insecure Operation*. Compromise of the IT assets 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 accounting 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.BADMEDIA *Corrupted Storage Media*. Corruption of storage media may cause security related data, such as database control data and accounting data, to be lost or corrupted. Storage media include on-line storage (e.g. for database files and on-line transaction logs) and off-line or archival storage (e.g. for database backups and audit archives). Such failures may arise from aging of storage media, or from improper storage or handling of removable 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.

T.TRUSTED *Abuse of Privilege by Trusted Users*. The IT assets cannot be reliably protected by the TOE from highly trusted users who abuse the privileges they are granted. This limits the scope of the threat T.ABUSE defined in the preceding section. Procedural measures are required to ensure that these highly trusted users can indeed be trusted not to abuse their privileges.

3.2 Organisational Security Policies

P.ACCESS Access rights to specific data objects are determined by:

a) the owner of the object; and

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

c) the implicit and explicit access rights to the object granted to the subject by the object owner.

3.3 Secure Usage Assumptions

3.3.1 Connectivity Assumptions

A.OS The TOE relies on an underlying operating system and/or secure network services that is installed and operated in a secure manner, i.e. in accordance with the operational documentation for the relevant products and any Certification Reports for those products.

A.NETWORK In a distributed environment the underlying network services must be based on secure communications protocols which ensure the authenticity of users.

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

A.FILES All of the database-related files and directories (including executables, run-time libraries, database files, export files, redo log files, control files, trace files, and dump files) are protected from unauthorised access by the operating system DAC mechanisms.

3.3.2 Physical Assumptions

A.LOCATE The processing resources of the TOE, the underlying operating system and/or underlying network services are located within controlled access facilities which will prevent unauthorised physical access.

A.PROTECT The hardware and software critical to security policy enforcement is physically protected from unauthorised modification by potentially hostile outsiders.

3.3.3 Personnel Assumptions

A.ACCESS The underlying operating system and/or secure network services are configured such that only the approved group of users for which the system is to be accredited has access to the system.

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

4 Security Objectives

4.1 IT Security Objectives

21 This section defines the IT security objectives that are to be satisfied by the TOE in combination with the IT security environment.

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

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

O.ACCESS The TOE must provide end-users and administrators with the capability of controlling and limiting access, by identified 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.DO The TOE must prevent the unauthorised or undesired disclosure, entry, modification, or destruction of data and data objects, in order to allow users who own or are responsible for data to control the access to that data by other authorised database users.

O.ACCESS.DA The TOE must prevent the unauthorised or undesired disclosure, entry, modification, or destruction of specified aggregations of data.

O.ACCESS.DC The TOE must prevent the unauthorised or undesired disclosure, entry, modification, or destruction of database control data or database accountability data.

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

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 IT assets open to compromise; and

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

O.RESOURCE The TOE must provide the means of controlling the consumption of global resources by specified users of the TOE, including the number of concurrent sessions.

O.ADMIN The TOE, where necessary in conjunction with the underlying operating 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 Non-IT Security Objectives

23 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 a manner which maintains IT security.

b) The underlying operating system and/or secure network services are installed and operated in accordance with the operational documentation for the relevant products. If the relevant products are certified they should be installed and operated in accordance with the appropriate operational documentation as listed in the Certification Report(s) and in accordance with the Evaluated Configuration of the product(s) (specifically, in accordance with any restriction on the use of product features and functions), and with any physical, procedural and personnel security measures specified by the Certification Report(s).

This objective counters threat T.OPERATE and maps onto environmental assertions A.OS and A.MANAGE.

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.

This objective counters threat T.PHYSICAL and maps onto environmental assertions A.ACCESS, A.PEER, A.LOCATE and A.PROJECT.

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 should 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 should be protected from unauthorised modification (so that the integrity of the audit timestamps is not compromised).

This objective supports the IT objective O.AUDIT in countering the identified threats.This objective is mapped onto environmental assertions A.MANAGE and A.FILES.

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.

This objective counters threat T.CRASH and maps onto environmental assertion A.MANAGE.

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 rights;

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

This objective supports IT objective O.RESOURCE in countering the identified threat and maps onto environmental assertion A.MANAGE.

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 or modify users and roles.

This objective counters threat T.TRUSTED and supports organisational security policy P.ACCESS. It maps onto environmental subsystem A.MANAGE.

O.AUTHDATA Those responsible for the TOE must ensure that the authentication data for each user account for the underlying operating system and/or secure network services 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 must not be physically removable from the underlying platform by unauthorised users;

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

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

This objective supports the IT objective O.I&A in countering the identified threats and supports organisational security policy P.ACCESS. In addition, it maps onto environmental assertions A.MANAGE, A.FILES, A.PEER and A.NETWORK.

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.

This objective counters threat T.BADMEDIA and maps onto environmental assertion A.MANAGE.

5 IT Security Requirements

5.1 TOE IT Security Functional Requirements

24 The following table lists the functional components included in this PP.

Component	Name
FIA_UID.1	Timing of Identification (*refined*)
FIA_ATD.1	Unique User Attribute Definition
FIA_USB.1	User-Subject Binding
FDP_ACC.1	Subset Object Access Control
FDP_ACF.1	Single Security Attribute Access Control
FDP_RIP.1	Subset Residual Information Protection
FMT_MSA.1	Basic User Attribute Administration
FMT_MSA.3	Static Attribute Initialisation
FMT_MTD.1	Management of TSF data
FMT_SMR.1	Security Management Roles
FMT_REV.1	Basic Revocation
FRU_RSA.1	Maximum Quotas
FTA_MCS.1	Basic Limitation on Multiple Concurrent Sessions
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Generation
FAU_SAR.1	Audit Review
FAU_SAR.3	Selectable Audit Review
FAU_SEL.1	Selective Audit
FAU_STG.1	Permanent Audit Trail Storage

Table 1: List of Security Functional Components

5.1.1 Identification and Authentication

FIA_UID.1.1 The TSF shall allow [assignment: *list of actions specified by the ST author*] 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.

25 *Note: FIA_UID.1 and FIA_UID.2 were integrated into FIA_UID.2 as the concept of* ***unique*** *identification of users was no longer recognised in the CC. FIA_UID.3 has become FIA_UID.1 as this was observed to provide a more secure generic set of controls over actions permitted before identification occurred.*

FIA_ATD.1.1 The TSF shall maintain *privileges, roles, resource limits* [assignment: *additional security attributes as specified by ST author*] belonging to individual users.

Note: It is necessary to maintain a set of privileges, roles and resource limits for each user in order to support the SFRs in this PP, other security attributes (for example authentication credentials) may be required.

Note: part of the functionality provided by FIA_ATD and FIA_ATA have been moved to the new FMT class.

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

5.1.2 Security Attribute Based Access Control

FDP_ACC.1.1 The TSF shall enforce the *database object access control SFP* on:

a) *subjects*;

b) *named objects*;

c) *all permitted operations on named objects by a subject.*

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

a) *the identity of the user associated with the database session and the privileges (user or object specific) which are effective for the database session*;

b) *the identity of the owner of the object and the object privileges which have been granted on the object*.

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

a) *if the user is the owner of the object then the requested access is allowed*;

b) *if the database session has the necessary object privileges effective for the object then the requested access is allowed*;

c) *if the user has a privilege enabling override of the object access controls then the requested access is allowed*;

d) otherwise access is denied.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the allocation of a resource to [assignment: *list of objects specified by the ST author*].

5.1.3 Security Management

FMT_MSA.1.1 The TSF shall enforce the *database object access control* SFP to:

a) restrict the ability to modify the values of the user attributes to only the authorised administrator;

b) provide authorised users with the ability to modify *object privileges*.

Refinement: object privileges can only be modified by the owner of the object or by a user who has an appropriate user privilege.

26 *Note: This SFR has to cover two cases, the management of user attributes and the management of object attributes. Hence the changes of wording and the introduction of a list.*

FMT_MSA.3.1 The TSF shall enforce the *database object access control SFP* to provide *restrictive* default values for object security attributes that are used to enforce the *database object access control SFP*.

FMT_MSA.3.2 The TSF shall allow *no users* to specify alternate initial values to override the default initial values when an object is created.

27 *Note: FDP_ACI.1 has been moved to the new FMT family.*

28 *Note: Object protection can be made more permissive in accordance with FDP_SAM.2. CCOR 823 has been raised requesting an additional component level within the FDP_ACI (now FMT_MSA) family specifying only the SFR stated above.*

FMT_MTD.1.1 The TSF shall restrict:

a) full access to the audit trail to the authorised administrator;

b) the ability to *read* the *audit records relating to objects owned by the user* to the authorised user.

29 *Note: part a) has been introduced to the SFR to cover unrestricted administrative access to the audit trail.*

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attibutes with the *users and objects* within the TSC to *authorised administrators (users and objects) and authorised users (for the objects they own or objects for which they have been granted sufficient privileges allowing them to revoke security attributes).*

FMT_REV.1.2 The TSF shall enforce revocation *in accordance with the following rules:*

a) revocation of object privileges shall take immediate effect on all new attempts to establish access to that object;

b) revocation of user privileges shall take effect when the user begins the next database session.

30 *Note: the above rules should be regarded as a minimum. A TOE which enforces*

stronger revocation rules in certain circumstances (e.g. immediate revocation) is still compliant with the above SFR.

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *set of roles supplied by the ST author*].

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

5.1.4 Resource Utilisation

FRU_RSA.1.1 The TSF shall enforce quotas limiting the maximum quantity of [assignment: *controlled database resources specified by the ST author*] that *an individual user* can use *during a database session*.

5.1.5 TOE Access

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 a single session per user.

31 *Note: it is acceptable for the limit to be configurable, and to rely on procedural measures to configure the limit in accordance with FTA_MCS.1.2.*

5.1.6 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 audit functions;

b) All auditable events for the *basic* level of audit; and

c) [assignment: *other auditable events as specified by the ST author*].

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, and *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, *other audit relevant information as identified in Table 2 below*.

Component	Event	Additional Information
FAU_PRO.2	All requests to read, modify or destroy the audit trail	-
FAU_SEL.2	All modifications to the audit configuration that occur while the audit collection functions are operating	-
FDP_ACF.1	All requests to perform an operation on an object covered by the SFP	-

Table 2: Required Auditable Events

Component	Event	Additional Information
FMT_MSA.1	All attempts to modify security attributes	Identity of the target of the modification attempt
FMT_MSA.1	All requests to use the user attribute administration functions	Identification of the user attributes modified
FMT_MSA.3	Any changes or overriding of the default object attributes	Identification of the default object attributes changed or overridden
FIA_UID.1	All attempts to use the user identification mechanism	User identity provided
FMT_SMR.1	Use of a security-relevant administrative function	-
FTA_MCS.1	All attempts at establishment of a user session	-

Table 2: Required Auditable Events

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

FAU_SAR.1.1 The TSF shall provide *authorised users* with the capability to read the audit data.

32 *Note: for a database audit trail SQL may be the tool of choice, for an OS audit trail this would be provided by the host operating system.*

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

FAU_SAR.3.1 The TSF shall provide the ability to perform searches and sorting of audit data based on [assignment: *multiple criteria with logical relations as specified by the ST author*].

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

a) *Event Type*;

b) [assignment: *list of additional attributes specified by the ST author*] that audit selectivity is based upon.

FAU_SEL.1.2 The TSF shall provide only the authorised administrator with the ability to select which events are to be audited.

FAU_STG.1.1 The TSF shall store generated audit records in a permanent audit trail.

5.2 IT Assurance Requirements

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

5.3 Security Requirements for the IT Environment

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

- **O.I&A**. The OS shall identify and authenticate users prior to providing access to any TOE facilities (*where required by the TOE*, although it is highly likely that other OS mechanisms will require this functionality in order to be effective).
- **O.ACCESS**. The OS shall provide the access control mechanisms required to support A.FILES and A.NETWORK. In addition these mechanisms are required to support O.AUTHDATA and O.ADMIN.
- **O.AUDIT & O.AUDITLOG**. The OS shall provide an audit mechanism and associated audit management tools to support the TOE, particularly in the case where the OS mechanisms are used to authenticate users, or the database audit trail is being written to the OS audit trail rather than a database table. To ensure the accuracy of the timestamps in both the database and OS audit trails the audit trail the OS should support FPT_STM.1.
- **O.RESOURCE**. The OS 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 OS shall provide backup, restore and other secure recovery mechanisms.

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

36 In addition to the above the OS shall provide mechanisms to ensure that the OS security functions are always invoked prior to passing control to the TOE and that non TOE activity within the OS does not interfere with the operation of the TOE. Thus the OS shall support FPT_RVM.1 and FPT_SEP.1 (at least).

37 A target assurance level of at least EAL3.

38 It is intended that the above requirements should be satisfied by an OS meeting the functional and assurance requirements as defined in the Controlled Access (C2) Protection Profile.

5.4 Minimum Strength of Function

39 The minimum strength of function for this Protection Profile is *medium*.

6 PP Application notes

6.1 Transaction Concurrency and Integrity

40 Early drafts of this PP contained a generic threat against database integrity, however it became clear that the rollback function FDP_ROL in CC Part 2 was inadequate of itself to counter this threat.

41 We did not wish however, to embark on a full scale implementation of all the additional SFRs which would be needed to counter a generic threat, addressing for example:

- referential integrity;
- transaction atomicity; *and*
- database recovery.

42 These issues have not yet featured in a security evaluation to date and it was felt inappropriate to introduce them at this time. Therefore the threat, objective and FDP_ROL SFR have been deleted from this issue.

43 We recommend that (in the absence of appropriate functionality in Part 2 of the CC) the ST author considers carefully whether to include appropriate IT security functions and SFRs written using CC Part 2 functional components ‘as a model for presentation’ (as per ASE_REQ.1.6C in CC Part 3).

7 Rationale

7.1 Security Objectives Rationale

44 This section provides a demonstration of why the identified security objectives (section 3) are suitable to counter the identified threats and meet the stated security policies (section 2).

45 The table below correlates the IT 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. In Table 3, a *YES* indicates that the identified IT security objective is relevant to the identified threat or security policy.

	O.I&A	**O.ACCESS**	**O.AUDIT**	**O.RESOURCE**	**O.ADMIN**
T.ACCESS	YES	YES			YES
T.DATA	YES	YES			YES
T.RESOURCE	YES			YES	YES
T.ATTACK	YES		YES		YES
T.ABUSE	YES		YES		YES
P.ACCESS		YES			

Table 3: Correlation of Threats and Policies to Objectives

46 T.ACCESS *Unauthorised Access to the Database* is directly countered by O.I&A 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 ensures the TOE, in conjunction with the underlying operating system, has the means of authenticating the claimed identity of any user. O.ACCESS.DC and O.ADMIN provide support by controlling access to database control data and administrative functionality that might otherwise enable circumvention of database access controls.

47 T.DATA *Unauthorised Access to Information* is directly countered by O.ACCESS.DO, O.ACCESS.DA and O.ACCESS.RD. O.ACCESS.DO ensures access is controlled to information contained within specific database objects. O.ACCESS.DA ensures access is controlled to specified aggregations of data. O.ACCESS.REUSE ensures access is prevented to residual information held in memory or reused database objects. O.I&A provides support by providing the means of identifying the user attempting to access a database object. O.ACCESS.DC and O.ADMIN provide support by controlling access to database control data and administrative functionality that might otherwise enable circumvention of database object access controls.

48 T.RESOURCE *Excessive Consumption of Resources* is countered directly by O.RESOURCE, which ensures the TOE has the means of limiting the consump-

tion of such resources, including the enforcement of limits on the number of concurrent sessions an individual may have. O.I&A provides support by providing the means of identifying the user attempting to use resources. O.ACCESS.DC and O.ADMIN provide support by controlling access to database control data and administrative functionality that might otherwise enable circumvention of resource utilisation controls.

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

50 T.ABUSE *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 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.DC and O.ADMIN provide support by controlling access to audit configuration data which only highly trusted individuals must be allowed to view and modify.

51 P.ACCESS is directly satisfied by O.ACCESS.DA and O.ACCESS.DO, which require provision of an access control policy as defined by P.ACCESS.

7.2 Security Requirements Rationale

7.2.1 Suitability of Security Requirements

52 Table 4 below 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.

	O.I&A	O.ACCESS	O.AUDIT	O.RESOURCE	O.ADMIN
FIA_UID.1	YES				
FIA_ATD.1	YES	YES		YES	YES
FIA_USB.1	YES	YES	YES	YES	YES
FDP_ACC.1		YES			
FDP_ACF.1		YES			
FDP_RIP.1		YES			

Table 4: Correlation of Objectives to Security Functional Requirements

	O.I&A	O.ACCESS	O.AUDIT	O.RESOURCE	O.ADMIN
FMT_MSA.1	YES	YES			YES
FMT_MSA.3		YES			
FMT_MTD.1			YES		
FMT_SMR.1					YES
FMT_REV.1		YES			
FRU_RSA.1				YES	
FTA_MCS.1				YES	
FAU_GEN.1			YES		
FAU_GEN.2			YES		
FAU_SAR.1			YES		
FAU_SAR.3			YES		
FAU_SEL.1			YES		
FAU_STG.1			YES		

Table 4: Correlation of Objectives to Security Functional Requirements

53 O.I&A is directly provided by FIA_UID.1 which provides the means of identifying users of the TOE. Identification and authentication checks are performed by the underlying operating system, as is protection of the authentication data. FIA_ATD.1 provides a unique set of user attributes for each user whilst FMT_MSA.1 specifies controls over the modification of these attributes. Finally, FIA_USB.1 provides an association between these user security attributes with subjects acting on behalf of the user.

54 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. FDP_ACI.1 ensures objects are protected by default from unauthorised access, thus ensuring no ‘window of opportunity’ is presented to an attacker when a new object is created. FDP_SAM.1 provides the means of controlling modification of the object security attributes, and FMT_REV.1 enforces revocation of those security attributes. FDP_RIP.1 ensures prevention of access to information residing in reused storage objects when they are re-allocated to another subject. Finally, 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.

55 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. FAU_STG.1 provides permanent storage for the audit trail whilst FMT_MTD.1 provides for protection of that audit trail. FAU_SAR.1 and FAU_SAR.3 provide functions to review the con-

tents of the audit trail, whilst FAU_SEL.2 provides the ability to select which events are to be audited.

56 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.

57 O.ADMIN is directly provided by FMT_SMR.1, which provides essential administrative functionality which is restricted to authorised administrators. 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. FIA_ATA.1 is also relevant, providing the administrator with the means of initialising user security attributes.

7.2.2 Dependency Analysis

58 The following table demonstrates that all dependencies of functional components are satisfied (note that '(H)' indicates the dependency is satisfied through the inclusion of a component that is hierarchical to the one required).

Component Reference	Component	Dependencies	Dependency Reference
1	**FIA_UID.1**	-	-
2	**FIA_ATD.1**	-	-
3	**FIA_USB.1**	FIA_ATD.1	2
4	**FDP_ACC.1**	FDP_ACF.1	5
5	**FDP_ACF.1**	FDP_ACC.1 FMT_MSA.3	4 8
6	**FDP_RIP.1**	-	-
7	**FMT_MSA.1**	FDP_ACC.1 FMT_SMR.1	4 11
8	**FMT_MSA.3**	ADV_SPM.1 FMT_MSA.1 FMT_SMR.1	note a) 7 11
9	**FMT_MTD.1**	FMT_SMR.1	11
10	**FMT_REV.1**	FMT_SMR.1	11

Table 5: Functional Component Dependency Analysis

Component Reference	Component	Dependencies	Dependency Reference
11	**FMT_SMR.1**	FIA_UID.1	1
12	**FRU_RSA.1**	-	-
13	**FTA_MCS.1**	FIA_UID.1	1
14	**FAU_GEN.1**	FPT_STM.1	see note b)
15	**FAU_GEN.2**	FAU_GEN.1 FIA_UID.1	14 1
16	**FAU_SAR.1**	FAU_GEN.1	14
17	**FAU_SAR.3**	FAU_SAR.1	16
18	**FAU_SEL.1**	FAU_GEN.1	14
19	**FAU_STG.1**	FAU_GEN.1	14

Table 5: Functional Component Dependency Analysis

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

a) ADV_SPM.1 is not an EAL3 assurance component, and therefore this dependency has been omitted. Note that because FMT_MSA.3 is a dependency of FDP_ACF.1 this would appear to rule out evaluating anything with access control below EAL4! A CCOR has been raised (#1246), which the CCIB appear to have accepted;

b) 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. Accordingly the IT environment section has been updated to include this requirement.

60 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.

7.2.3 Demonstration of Mutual Support

61 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. 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.2, FMT_MTD.1, FAU_SAR.1 and FAU_SEL.1.

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

c) FDP_ACI.1 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 supports FAU_GEN.1 by providing permanent storage for the audit trail.

g) FMT_MTD.1 supports FAU_STG.1 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.

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

7.3 Strength of Functions Rationale

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

7.4 Security Assurance Rationale

64 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 targetted at the 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.

65 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.