Oracle AI Database 26ai
Security Target

Version: 1.1
Date: 2025-12-17

Oracle Corporation
2300 Oracle Way
Austin, TX 78741
U.S.A.

Prepared by:

Combitech AB
351 80 Växjö
Sweden

DOCUMENT HISTORY

Version	Status	Issue date	Revision description	Edited by
0.1	Draft	2024-02-01	First draft version	Anders Staaf
0.2	Draft	2024-02-16	Updated after comments from Oracle	Anders Staaf
0.3	Draft	2024-02-20	Updated after comments from Oracle	Anders Staaf
0.4	Draft	2024-02-21	Updated after comments from Oracle	Anders Staaf
0.5	Draft	2024-03-25	Addressing the evaluator's observations. Changed the fourth bullet in section 1.6.4.	Anders Staaf
0.6	Draft	2024-06-17	TOE name changed to Oracle Database 23ai. Addressed the certifier's comments.	Anders Staaf
0.7	Draft	2025-09-09	VPD removed. Platform changed to Exadata. Adopted TD001 and TD002	Anders Staaf
0.8	Draft	2025-10-07	Updated after comments from Oracle	Anders Staaf
0.9	Draft	2025-10-16	TOE name changed to Oracle AI Database 26ai	Anders Staaf
1.0	Approved	2025-12-09	Only the version is changed, for the ST to be published.	Anders Staaf
1.1	Approved	2025-12-17	Updated after review of Certification Report	Anders Staaf

Contents

1 ST Introduction

1.1 ST Reference

Title: Oracle AI Database 26ai Security Target

Version: 1.1

Date: 2025-12-17

Editor: Anders Staaf, Combitech AB

1.2 TOE Reference

TOE: Oracle AI Database 26ai

Version: AI Database 26ai (23.26.0) with Critical Patch Update October 2025

Date: 2025-10-21

Developer: Oracle Corporation

1.3 Document Overview

Chapter 1 gives a description of the ST and the TOE. This description serves as an aid to understand the security requirements and the security functions.

Chapter 2 states the conformance claims made.

Chapter 3 describes the security problem definition of the TOE. This includes assumptions about the environment of the TOE, threats against the TOE, TOE environment and organizational security policies that are to be employed to ensure the security of the TOE.

Chapter 4 describes the Security Objectives stated in the intent of the Security Functions. The Security Objectives are divided into two groups of security objects, for the TOE and for the TOE environment.

Chapter 5 defines the extended components which are then detailed in Section 6.

Chapter 6 specified the IT security functional and assurance requirements that must be satisfied by the TOE.

Chapter 7 describes how the security functional requirements are implemented in the TOE.

1.4 Conventions

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2, are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item].
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish

between iterations, e.g., ‘FDP_ACC.1(1), Subset access control (administrators)’ and ‘FDP_ACC.1(2) Subset access control (devices)’.

1.5 TOE Overview

Oracle AI Database 26ai is a relational database management system (DBMS) from the Oracle Corporation. The system is built around a relational database framework in which data objects may be directly accessed by users, or an application front end, through structured query language (SQL). Oracle is a fully scalable, multitenant, relational database architecture typically used by global enterprises and governments to manage and process data across wide and local area networks.

The security functionality in Oracle AI Database 26ai includes:

- Configurable audit capture.
- Fine-grained access controls on database objects. Discretionary Access Control (DAC) is based on object, schema, and system privileges, as well as roles. Fine-grained access control may be implemented to allow access based on the information itself. For example, a user may be granted access to their own human resources details, but not the details of the other users contained in the same tables.
- User identification and authentication. Users are identified and authenticated before access to database objects is allowed. On login, the user identity is associated with role and privilege information that is used to make access control decisions.
- Security management functionality. The security functionality associated with audit, access control, and user accounts are provided through the SQL command line interface (CLI).
- Consistent replication. The content of a database may be replicated to another server, with assurances that the consistency of the data is maintained.

The TOE is a software only TOE.

1.6 TOE Description

1.6.1 Physical Scope

The TOE consists of the Oracle AI Database 26ai software in one of the four configurations shown in Figure 1.

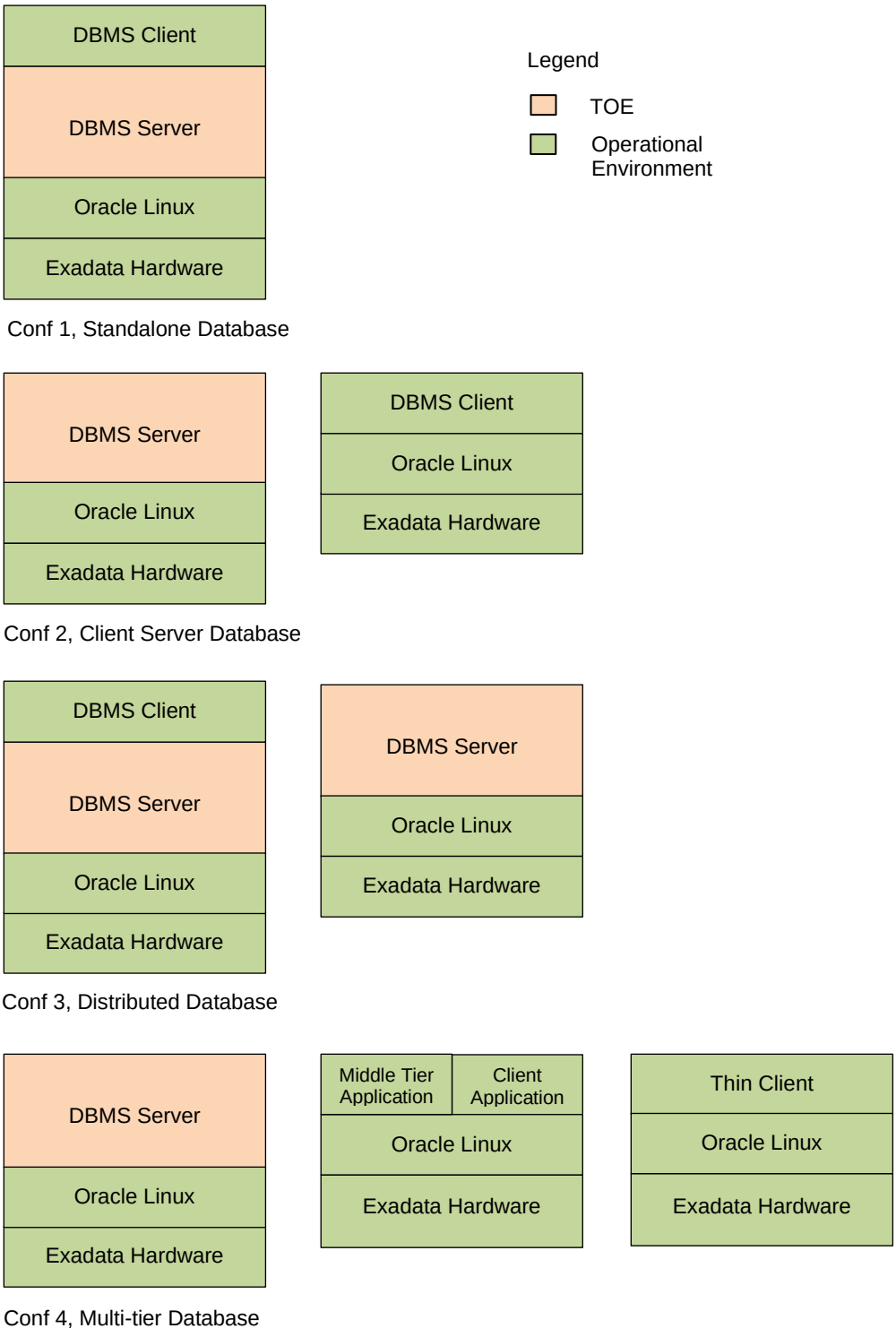

Figure 1, TOE configurations

The configurations are:

1. The DBMS server operated with a co-located client
2. The DBMS server operated with a remote client

3. A primary DBMS server and a secondary DBMS server with replicated data
4. A DBMS server accessed by a thin client through a middle tier application proxy

1.6.1.1 TOE Delivery

Oracle Exadata platform ships with the Oracle Linux operating system installed on the servers.

Oracle strongly recommends that customers purchase the install service of the Exadata database machine from Oracle or our certified service partners. The installation is performed using the Oracle Exadata Deployment Assistant. The installation and configuration are described in *Oracle® Exadata Database Machine Installation and Configuration Guide for Exadata Database Machine.*

1.6.1.2 TOE Guidance

The TOE includes the following guidance documentation:

- Oracle® Exadata Database Machine, Installation and Configuration Guide for Exadata Database Machine, 25.2 F29249-41, October 2025
- Oracle® AI Database, Database Installation Guide, 26ai for Linux, G43069-01, October 2025
- Oracle® AI Database, Database Administrator's Guide, 26ai G42927-01, October 2025
- Oracle® AI Database, Multitenant Administrator's Guide, 26ai G43631-01, October 2025
- Oracle® AI Database, SQL Language Reference, 26ai G43935-01, October 2025
- Oracle® AI Database, Database PL/SQL Language Reference, 26ai G43964-01, October 2025
- Oracle® AI Database, Security Guide, 26ai G43025-02, October 2025
- Oracle® AI Database, Data Guard Concepts and Administration, 26ai G43580-01, October 2025

These documents may be downloaded from the Oracle web site, https://docs.oracle.com/en/database/oracle/oracle-database/index.html

The following document is available from https://www.oracle.com/corporate/security-practices/assurance/development/external-security-evaluations/common-criteria/certifications/:

- Oracle AI Database 26ai, Common Criteria Guidance Supplement, Version 0.7, 2025-10-16

1.6.2 Non-TOE Hardware/Software/Firmware

The following operating system and hardware components are required for operation of the TOE in the evaluated configuration.

Component	Operating System	Hardware
Oracle AI Database 26ai (TOE component)	Oracle Enterprise Linux 8	Exadata X11M

Component	Operating System	Hardware
Oracle AI Database 26ai, second instance (TOE component)	Oracle Enterprise Linux 8	Exadata X11M
Database client (Non-TOE component)	Oracle Enterprise Linux 8	Exadata X11M

Table 1, Operational Environment Operating System and Hardware Requirements

Note that the Database client refers to the presentation of the SQL commands at the TOE interface. These are the same whether they are entered on the database machine, from a client machine or from an application.

1.6.3 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in chapter 6. Table 2 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	Audit entries are generated for security related events. Audit policies may be created to generate logs based on details such as the user, the object being accessed, event type or success or failure of the operation.
User Data Protection	The TOE provides a discretionary access control policy to provide fine-grained access control between users and database objects. The TOE provides a multitenant environment where resources in pluggable databases are logically separate and inaccessible by local users in any other pluggable database or Container Database (CDB). Once data is allocated to a resource, the previous information content is no longer available.
Identification and Authentication	Users must identify and authenticate prior to gaining TOE access. Attributes are maintained to support the access control policy.
Security Management	The TOE provides management capabilities via SQL statements. Management functions allow the administrators to: • configure auditing and access control options (including granting and revoking privileges) • configure users (including the maximum number of concurrent sessions) and roles • configure replication options • configure separate domains for pluggable databases within a container database • assess roles and privileges in use at run-time

Functional Classes	Description
Protection of the TSF	Data may be consistently replicated to a secondary DBMS server.
TOE Access	The number of concurrent user sessions may be limited by policy. User login may be restricted based on user identity.

Table 2, Logical Scope of the TOE

1.6.4 Functionality Excluded from the Evaluated Configuration

The following features are excluded from this evaluation:

- Authentication features
    - Although Oracle AI Database 26ai supports several authentication mechanisms, including Kerberos and Public Key Infrastructure, only Oracle password authentication was demonstrated for the purposes of this evaluation.
- Real Application Clusters (RAC)
- External clients
- DBaaS databases
    - Oracle Cloud Infrastructure (OCI) DBaaS databases which is the Oracle Database deployed in the cloud and offered as a service, were not evaluated.
- Database Vault
    - Oracle Database Vault adds mandatory access controls within the Oracle AI Database that restrict access to specific schemas, objects, and SQL operations regardless of system or DBA privileges, with enforcement handled by the database kernel. These controls are implemented using realms to protect database objects, command rules to govern execution of SQL statements, and secure application roles that are enabled only under defined conditions. Database Vault was not evaluated..
- Oracle Label Security
    - Oracle Label Security (OLS), controls the display of data within a table using labels that are assigned to data objects and to application users. When access is requested, OLS compares the data label with the user's label authorizations. Access to specific data objects can be restricted based on authorization level, compartments and groups. OLS was not evaluated.

2 Conformance Claims

2.1 CC Conformance Claim

This Security Target and TOE claims to be conformant to Common Criteria version 3.1 according to:

- Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
    - Part 2 extended
- Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017
    - Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 has been taken into account.

2.2 PP Conformance Claims

This Security Target claims exact conformance with the collaborative Protection Profile for Database Management Systems, 13 March 2023, Version 1.3 (cPP DBMS).

The supporting document Evaluation Activities for the collaborative Protection Profile for Database Management Systems, 15 March 2023, Version 1.1 (SD DBMS) has been taken into account.

The following Technical Decisions have been taken into account:

Technical Decision TD_DBMS_B_001 *Update to Role Definitions and Security Attribute Management for Consistency*,

Technical Decision TD_DBMS_B_002: *Session Locking Mechanism Expansion*

The Technical Decisions are published at the DBMS iTC site: https://dbms-itc.github.io/

2.3 Package Conformance Claims

This Security Target claims conformance to assurance requirement package EAL2 augmented by ALC_FLR.3, Flaw Reporting Procedures.

2.4 Conformance Rationale

The security problem definition and security objectives have been drawn from the claimed Protection Profile, cPP DBMS.

All of the mandatory Security Functional Requirements (SFRs) from the cPP DBMS have been included as well as the selection-based and optional SFRs:

a) FIA_USB.2_EXT Enhanced user-subject binding;
b) FPT_TRC.1 Internal TSF consistency;
c) FCS_MCS_EXT.1 Configurable session limiting mechanisms;

d) FCS_MCS.1 Concurrent Session Control; and
e) FTA_TAH.2_EXT TOE access information

Application Note: The security requirement stated in FIA_USB.2_EXT is equal to the security requirement stated in the SFR component FIA_USB.2_EXT defined in DBMS cPP [5].

3 Security Problem Definition

3.1 Introduction

The security problem definition described below includes threats, organisational security policies and security usage assumptions.

3.2 Informal Discussion

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

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

3.3 Assets and Threat Agents

The threats given in section 3.4 refer to various threat agents and assets. The term "threat agent" is defined in CC Part 1.

The assets, mentioned in Table 3, are either defined in CC Part 1, or in the glossary in Appendix B – Terms and Definitions.

The terms "TSF data", "TSF" and "user data", are defined in CC Part 1. The terms "public objects" and "TOE resources" are given in the glossary in Appendix B – Terms and Definitions.

3.4 Threats

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

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

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

Table 3, Threats Applicable to the TOE

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

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

Table 4: Policies Applicable to the TOE

3.5 Assumptions

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

Assumption	Definition
Physical aspects	

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

Table 5: Assumptions Applicable to the TOE Environment

4 Security Objectives

4.1 Introduction

The statement of security objectives defines the security objectives for the TOE and its environment. The security objectives intend to address all security environment aspects identified. The security objectives reflect the stated intent and are suitable to counter all identified threats and cover all identified organisational security policies and assumptions. The following categories of objectives are identified:

- The security objectives for the TOE shall be clearly stated and traced back to aspects of identified threats to be countered by the TOE and/or organisational security policies to be met by the TOE.

- The security objectives for the environment shall be clearly stated and traced back to aspects of identified threats countered by the TOE environment, organisational security policies or assumptions.

4.2 Security Objectives for the TOE

The following security objectives are defined for the TOE.

Security Objective	Description
O.ADMIN_ROLE	The TOE shall provide roles that allow only authorized users to have access to administrative privileges that are specific to the role.
O.AUDIT_GENERATION	The TOE shall provide the capability to detect and create/generate records of security relevant events associated with users.
O.DISCRETIONARY_ACCESS	The TSF shall control access of subjects and/or users to named resources based on identity of the object, subject, or user. The TSF shall allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.
O.I&A	The TOE shall ensure that users are authenticated before the TOE processes any actions that require authentication.
O.MANAGE	The TSF shall provide all the functions and facilities necessary to manage TOE security mechanisms, and shall restrict such management actions to authorized users.
O.RESIDUAL_INFORMATION	The TOE shall ensure that any information contained in a protected resource within its control is not inappropriately disclosed when the resource is reallocated.
O.TOE_ACCESS	The TOE shall provide functionality that controls a user's logical access to user data and to the TSF.

Table 6, Security objectives for the TOE

4.3 Security Objectives for the Operational Environment

The following security objectives for the operational environment are defined for the TOE.

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

Table 7, Security objectives for the TOE operational environment

4.4 Security Objectives for the Operational IT Environment

The following security objectives for the operational IT environment are defined for the TOE.

Security Objective	Description
OE.IT_I&A	Any information provided by a trusted entity in the environment and used to support user authentication and authorization used by the TOE is correct and up to date.
OE.IT_TRUSTED_SYSTEM	External IT systems may be required by the TOE for the enforcement of the security policy. These external trusted IT systems shall be managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and are physically and shall be sufficiently protected from any attack that may cause those functions to provide false results.

Table 8, Security objectives for the TOE operational environment

4.5 Security Objectives Rationale

4.5.1 Security Objectives Coverage

This section provides tracings of the security objectives for the TOE to threats, OSPs, and assumptions.

	T.ACCESS_TSFDATA	T.ACCESS_TSFFUNC	T.IA_USER	T.RESIDUAL_DATA	T.UNAUTHORIZED_ACCESS	P.ACCOUNTABILITY	P.ROLES	P.USER	A.AUTHUSER	A.CONNECT	A.MANAGE	A.NO_GENERAL_PURPOSE	A.PEER_FUNC_&_MGT	A.PHYSICAL	A.SUPPORT	A.TRAINEDUSER
O.ADMIN_ROLE		X				X	X									
O.AUDIT_GENERATION						X										
O.DISCRETIONARY_ ACCESS			X		X											
O.I&A	X	X	X			X										
O.MANAGE	X	X			X			X								
O.RESIDUAL_ INFORMATION				X												
O.TOE_ACCESS	X	X	X		X	X	X	X								
OE.ADMIN								X			X					
OE.INFO_PROTECT					X			X	X	X	X			X		X
OE.NO_GENERAL_ PURPOSE												X				
OE.PHYSICAL										X				X		
OE.IT_I&A															X	
OE.IT_TRUSTED_ SYSTEM										X			X			

Table 9, Security objectives coverage

4.5.2 Sufficiency of the Security Objectives for the TOE

The following rationale provides justification that the security objectives for the TOE are suitable to cover each individual threat and OSP for the TOE.

Threat/OSP	Objective	Rationale
T.ACCESS_TSFDATA A user or a process may read or modify TSF data using functions of the TOE without being identified, authenticated and authorized.	O.I&A The TOE shall ensure that users are authenticated before the TOE processes any actions that require authentication.	O.I&A supports this policy by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE is defined to provide to authenticated users only.
	O.MANAGE The TSF shall provide all the functions and facilities necessary to manage TOE security mechanisms, and shall restrict such management actions to authorized users.	O.MANAGE diminishes this threat since it ensures that functions and facilities used to modify TSF data are not available to unauthorized users.
	O.TOE_ACCESS The TOE shall provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS mitigates this threat by restricting TOE access.
T.ACCESS_TSFFUNC A user or a process may use, manage or modify the TSF, bypassing the protection mechanisms of the TSF.	O.ADMIN_ROLE The TOE will provide roles that allow only authorized users to have access to administrative privileges that are specific to the role.	O.ADMIN_ROLE mitigates this threat by restricting access to privileged actions.
	O.I&A The TOE shall ensure that users are authenticated before the TOE processes any actions that require authentication.	O.I&A mitigates this threat since the TOE requires successful authentication to the TOE prior to gaining access to any controlled-access content.
	O.MANAGE The TSF shall provide all the functions and facilities necessary to manage TOE security mechanisms, and shall restrict such management actions to authorized users.	O.MANAGE mitigates this threat by ensuring that management functions are restricted to authorized users.
	O.TOE_ACCESS	O.TOE_ACCESS

Threat/OSP	Objective	Rationale
	The TOE shall provide mechanisms that control a user's logical access to user data and to the TSF.	mitigates this threat by restricting TOE access.
T.IA_USER A user who has not successfully completed identification and authentication may gain unauthorized access to user data or TOE resources beyond public objects.	O.DISCRETIONARY_ACCESS The TSF shall control access of subjects and/or users to named resources based on identity of the object, subject, or user. The TSF shall allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.	O.DISCRETIONARY_ACCESS mitigates this threat by requiring that data, including user data stored with the TOE, is protected by discretionary access controls.
	O.I&A The TOE shall ensure that users are authenticated before the TOE processes any actions that require authentication.	O.I&A mitigates this threat by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing access beyond public objects
	O.TOE_ACCESS The TOE shall provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS mitigates this threat by controlling logical access to user data and TSF data.
T.RESIDUAL_DATA A user or a process acting on behalf of a user may gain unauthorized access to user or TSF data through reallocation of TOE resources from one user or process to another.	O.RESIDUAL_INFORMATION The TOE shall ensure that any information contained in a protected resource is not inappropriately disclosed when the resource is reallocated.	O.RESIDUAL_INFORMATION mitigates this threat by ensuring that data is not improperly disclosed.
T.UNAUTHORIZED_ACCESS An authenticated user or a process, in conflict with the TOE security policy, may gain unauthorized access to user data.	O.DISCRETIONARY_ACCESS The TSF shall control access of subjects and/or users to named resources based on identity of the object, subject or user. The TSF shall allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.	O.DISCRETIONARY_ACCESS mitigates this threat by requiring that data, including TSF data, is protected by discretionary access controls.
	O.MANAGE The TSF shall provide all the functions and facilities necessary	O.MANAGE

Threat/OSP	Objective	Rationale
	to manage TOE security mechanisms, and shall restrict such management actions to authorized users.	mitigates this threat by ensuring that access to user data is restricted to authorized users.
	O.TOE_ACCESS The TOE shall provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS mitigates this threat by controlling logical access to user data and TSF data.
P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE.	O.ADMIN_ROLE The TOE shall provide roles that allow only authorized users to have access to administrative privileges that are specific to the role.	O.ADMIN_ROLE supports this policy by ensuring that the TOE provides a means of granting authorized administrators the privileges needed for secure administration.
	O.AUDIT_GENERATION The TOE shall provide the capability to generate records of security relevant events associated with users.	O.AUDIT_GENERATION supports this policy by ensuring that audit records are generated to enable accountability.
	O.I&A The TOE shall ensure that users are authenticated before the TOE processes any actions that require authentication.	O.I&A supports this policy by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action.
	O.TOE_ACCESS The TOE shall provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS supports this policy by providing a mechanism for controlling user access.
P.ROLES Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible while supporting only the administrative duties the person has. This role shall be separate and distinct from other authorized users.	O.ADMIN_ROLE The TOE shall provide roles that allow only authorized users to have access to administrative privileges that are specific to the role.	O.ADMIN_ROLE supports this objective by providing roles that allow only authorized users access to administrative privileges.
	O.TOE_ACCESS The TOE shall provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS supports this policy by controlling access to TSF functionality based on role.
	O.MANAGE	O.MANAGE

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

Table 10, Sufficiency of the security objectives for the TOE

4.5.3 Sufficiency of the Security Objectives for the Environment

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual threat, OSP, and assumption for the environment.

Threat/OSP/Assumption	Objective	Rationale
T.UNAUTHORIZED_ACCESS A user may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.	OE.INFO_PROTECT Those responsible for the TOE shall establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling shall be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate	OE.INFO_PROTECT diminishes the logical and physical threats by ensuring that the network and peripheral cabling are appropriately protected. DAC protections, when implemented correctly, support the identification of unauthorized access.

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

Threat/OSP/Assumption	Objective	Rationale
A.AUTHUSER Authorized users possess the necessary authorization to access the information managed by the TOE in accordance with organization information access policies.	OE.INFO_PROTECT Those responsible for the TOE shall establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling shall be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT diminishes the logical and physical threats by ensuring that the network and peripheral cabling are appropriately protected. DAC protections, when implemented correctly, support the identification of unauthorized access.
A.CONNECT All connections to and from remote trusted IT systems and between separate parts of the TSF are physically and/or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.	OE.INFO_PROTECT Those responsible for the TOE shall establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling shall be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit	OE.INFO_PROTECT diminishes the logical and physical threats by ensuring that the network and peripheral cabling are appropriately protected. DAC protections, when implemented correctly, support the identification of unauthorized access.

Threat/OSP/Assumption	Objective	Rationale
	trails and authorization databases) shall always be set up correctly. Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	
	OE.IT_TRUSTED_SYSTEM External IT systems may be required by the TOE for the enforcement of the security policy. These external trusted IT systems shall be managed according to known, accepted and trusted policies based on the same rules and policies applicable to the TOE, and shall be sufficiently protected from any attack that may cause those functions to provide false results.	OE.IT_TRUSTED_SYSTEM supports the assumption by ensuring that external trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy.
	OE.PHYSICAL Those responsible for the TOE shall ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection shall be commensurate with the value of the IT assets protected by the TOE.	OE.PHYSICAL supports the assumption by ensuring that appropriate physical security is provided within the domain.
A.MANAGE The TOE security functionality is managed by one or more competent, authorized administrators. The system administrative personnel are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.	OE.ADMIN Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of information it contains.	OE.ADMIN supports the assumption by requiring that authorized administrators are competent, thereby ensuring that all the tasks are performed correctly and effectively.
	OE.INFO_PROTECT Those responsible for the TOE shall establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling shall be approved for the transmittal of the most	OE.INFO_PROTECT diminishes the logical and physical threats by ensuring that the network and peripheral cabling are appropriately protected. DAC protections, when implemented correctly, support

Threat/OSP/Assumption	Objective	Rationale
	sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	the identification of unauthorized access.
A.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration, and support of the DBMS.	OE.NO_GENERAL_PURPOSE There shall be no general-purpose computing capabilities (e.g., compilers or user applications) available on DMBS servers, other than those services necessary for the operation, administration, and support of the DBMS.	OE.NO_GENERAL_PURPOSE The DBMS server must not include any general-purpose computing capabilities. This will protect the TSF data from malicious processes.
A.PEER_FUNC_&_MGT All external trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.	OE.IT_TRUSTED_SYSTEM External IT systems may be required by the TOE for the enforcement of the security policy. These external trusted IT systems shall be managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and shall be sufficiently protected from any attack that may cause those functions to provide false results.	OE.IT_TRUSTED_SYSTEM supports this assumption by ensuring that remote systems supporting the TOE are managed in a manner consistent with the security policies applicable to the TOE.
A.PHYSICAL The operational environment is assumed to provide the TOE with appropriate physical	OE.PHYSICAL Those responsible for the TOE shall ensure that those parts of the TOE critical to enforcement of the security policy are protected from	OE.PHYSICAL supports this assumption by ensuring that the parts of the TOE critical to the enforcement of

Threat/OSP/Assumption	Objective	Rationale
protection such that the TOE is not subject to physical attack that may compromise the security and/or interfere with the platform's correct operation. This includes protection for the physical infrastructure on which the TOE depends for correct operation and hardware devices on which the TOE is executing.	physical attack that might compromise IT security objectives. The protection shall be commensurate with the value of the IT assets protected by the TOE.	the security policy are protected from physical attack.
	OE.INFO_PROTECT Those responsible for the TOE shall establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling shall be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT diminishes the logical and physical threats by ensuring that the network and peripheral cabling are appropriately protected. DAC protections, when implemented correctly, support the identification of unauthorized access.
A.SUPPORT Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is used by the TOE is correct and up to date.	OE.IT_I&A Any information provided by a trusted entity in the environment and used to support user authentication and authorization used by the TOE is correct and up to date.	OE.IT_I&A supports the assumption implicitly.
A.TRAINEDUSER Authorized users are sufficiently trained to accomplish a task or	OE.INFO_PROTECT Those responsible for the TOE shall establish and implement	OE.INFO_PROTECT diminishes the logical and physical threats by ensuring that

Threat/OSP/Assumption	Objective	Rationale
group of tasks within a secure IT environment by exercising control over their user data.	procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling shall be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	the network and peripheral cabling are appropriately protected. DAC protections, when implemented correctly, support the identification of unauthorized access.

Table 11, Sufficiency of the security objectives for the environment

5 Extended Components Definition

5.1 User Identification and Authentication (FIA)

5.1.1 User-subject Binding (FIA_USB)

Family Behaviour

An authenticated user, in order to use the TOE, typically activates a subject. The user's security attributes are associated (totally or partially) with this subject. This family defines requirements to create and maintain the association of the user's security attributes to a subject acting on the user's behalf.

Component Levelling

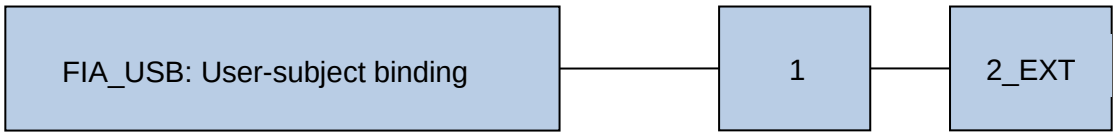

Figure 2, FIA_USB: User-subject binding component levelling

FIA_USB.2_EXT Enhanced user-subject binding is an extended SFR component modelled after FIA_USB.1 and added to the FIA_USB existing family. FIA_USB.2_EXT is analogous to FIA_USB.1 except that it adds the possibility to specify rules whereby subject security attributes are also derived from TSF data other than user security attributes. FIA_USB.2_EXT is hierarchical to FIA_USB.1.

Application Note: The security requirement stated in FIA_USB.2_EXT is equal to the security requirement stated in the SFR component FIA_USB_EXT.2 defined in DBMS cPP [5].

Management: FIA_USB.2_EXT

The following actions could be considered for the management functions in FMT:

a. an authorized administrator can define default subject security attributes.

b. an authorized administrator can change subject security attributes.

Audit: FIA_USB.2_EXT

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject).

b. Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).

FIA_USB.2_EXT Enhanced user-subject binding

Hierarchical to: FIA_USB.1 User-subject binding

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.2.1_EXT The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: list of user security attributes].

FIA_USB.2.2_EXT The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: rules for the initial association of attributes].

FIA_USB.2.3_EXT The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: rules for the changing of attributes].

FIA_USB.2.4_EXT **The TSF shall enforce the following rules for the assignment of subject security attributes not derived from user security attributes when a subject is created: [assignment: rules for the initial association of the subject security attributes not derived from user security attributes].**

5.2 TOE access (FTA)

5.2.1 Configurable Session Limiting Mechanisms (FTA_MCS_EXT)

Family Behaviour

This family defines requirements to configure mechanisms to limit the number of concurrent sessions.

Component Levelling

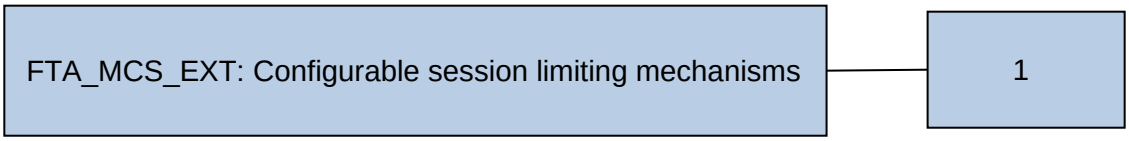

Figure 3, FTA_MCS_EXT: Configurable session limiting mechanisms component levelling

FTA_MCS_EXT Configurable session limiting mechanisms is an extended SFR family modelled after FTA_MCS. FTA_MCS_EXT.1 Configurable session limiting mechanisms is the only component within this family and provides the requirement for a TOE to configure session limiting mechanisms.

FTA_MCS_EXT.1 is not hierarchical to any other components.

Management: FTA_MCS_EXT.1

The following actions could be considered for the management functions in FMT:

a) select and configure the selected enforcement mechanisms.

Audit: FTA_MCS_EXT.1

There are no auditable events foreseen.

FTA_MCS_EXT.1 **Configurable session limiting mechanisms**

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_MCS_EXT.1.1: The TSF shall restrict the maximum number of concurrent sessions based on [selection: User session locking as defined by FTA_MCS.1, [assignment: *mechanism(s) for session limitation enforced by the TSF*]].

FTA_MCS_EXT.1.2: The TSF shall provide the capability for an authorized administrator to configure the selected enforcement mechanisms.

5.2.2 TOE access history (FTA_TAH)

Family Behaviour

This family defines requirements for the TSF to display to a user, upon successful session establishment, a history of successful and unsuccessful attempts to access the user's account.

Component Levelling

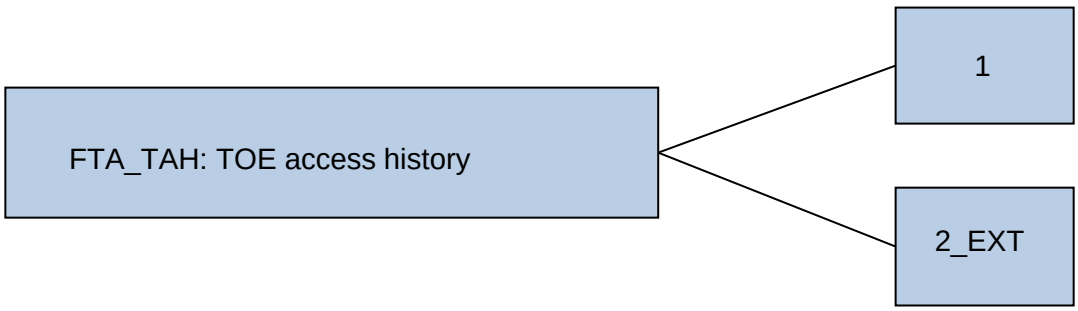

Figure 4, FTA_TAH: TOE access history component levelling

FTA_TAH.2_EXT TOE access information is an extended SFR component modelled after FTA_TAH.1 and added to this existing family. FTA_TAH.2_EXT provides the requirement for a TOE to make available information related to attempts to establish a session. FTA_TAH.2_EXT is not hierarchical to any other components.

Application Note: The security requirement stated in FIA_TAH.2_EXT is equal to the security requirement stated in the SFR component FTA_TAH_EXT.2 defined in DBMS cPP [5].

Management: FTA_TAH.2_EXT

There are no management activities foreseen.

Audit: FTA_TAH.2_EXT

There are no auditable events foreseen.

FTA_TAH.2_EXT **TOE access information**

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_TAH.2.1_EXT Upon a session establishment attempt, the TSF shall store

a) the date and time of the session establishment attempt of the user.

b) the incremental count of successive unsuccessful session establishment attempt(s).

FTA_TAH.2.2_EXT Upon successful session establishment, the TSF shall allow the date and time of

a) the previous last successful session establishment, and

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

to be retrieved by the user.

6 Security Functional Requirements

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SEL.1	Selective audit
User Data Protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_RIP.1	Subset residual information protection
Identification and Authentication (FIA)	FIA_ATD.1	User attribute definition
	FIA_UAU.2	Timing of authentication
	FIA_UID.2	Timing of identification
	FIA_USB.2_EXT	Enhanced user-subject binding
Security Management (FMT)	FMT_MSA.1(1)	Management of security attributes (Users)
	FMT_MSA.1(2)	Management of security attributes (Objects)
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_REV.1(1)	Revocation (Users)
	FMT_REV.1(2)	Revocation (Objects)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_TRC.1	Internal TSF consistency
TOE Access (FTA)	FTA_MCS.1	Basic limitation on multiple concurrent sessions
	FTA_MCS_EXT.1	Configurable session limiting mechanisms
	FTA_TAH.2_EXT	TOE access information
	FTA_TSE.1	TOE session establishment

Table 12, Security Functional Requirements

6.1 Security audit – FAU

6.1.1 Audit data generation – FAU_GEN

6.1.1.1 Audit data generation – FAU_GEN.1

Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

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

b) All auditable events for the [minimum] level of audit **listed in Table 13, Auditable events**; and

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

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

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, [*information specified in column three of Table 13, Auditable events, below*].

Column 1: **Security Functional Requirement**	**Column 2:** **Auditable Event(s)**	**Column 3:** **Additional Audit Record Contents**
FAU_GEN.1	None	None
FAU_GEN.2	None	None
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	The identity of the authorized administrator that made the change to the audit configuration
FDP_ACC.1	None	None
FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP	None
FDP_RIP.1	None	None
FIA_ATD.1	None	None
FIA_UAU.2	Unsuccessful use of the authentication mechanism	None
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided	The user identity provided
FIA_USB.2_EXT	Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject)	None
FMT_MSA.1(1)	None	None

Column 1: **Security Functional Requirement**	**Column 2:** **Auditable Event(s)**	**Column 3:** **Additional Audit Record Contents**
FMT_MSA.1(2)	None	None
FMT_MSA.3	None	None
FMT_MTD.1	None	None
FMT_REV.1(1)	Unsuccessful revocation of security attributes	Identity of individual attempting to revoke security attributes
FMT_REV.1(2)	Unsuccessful revocation of security attributes	Identity of individual attempting to revoke security attributes
FMT_SMF.1	Use of the management functions	Identity of the administrator performing these functions
FMT_SMR.1	Modifications to the group of users that are part of a role	Identity of authorized administrator modifying the role definition
FPT_TRC.1	Restoring consistency	None
FTA_MCS.1	Rejection of a new session based on the limitation of multiple concurrent sessions	None
FTA_MCS_EXT.1	None	None
FTA_TAH.2_EXT	None	None
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism	Identity of the individual attempting to establish a session

Table 13, Auditable events

6.1.1.2 User identity association – FAU_GEN.2

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users and **any identified groups**, the TSF shall be able to associate each auditable event with the identity of the **[**user**]** that caused the event.

6.1.1.3 Selective audit – FAU_SEL.1

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

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

a) user identity;

b) [object identity; event type; **success of auditable security events; failure of auditable security events**]

c) [*no additional attributes*].

Application Note: The audit functionality may be configured to audit specified operations. 'Event type' is defined to be these specified operations for the purposes of FAU_SEL.1.

6.2 User data protection – FDP

6.2.1 Access control policy - FDP_ACC

6.2.1.1 Subset access control – FDP_ACC.1

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [*Discretionary Access Control Policy*] on [*all subjects, all DBMS-controlled objects, and all operations among them*].

6.2.1.2 Security attribute based access control – FDP_ACF.1

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [*Discretionary Access Control Policy*] to objects based on the following:

[*Subjects: Database users;*
Subject attributes: User identity, database role, schema privileges, system privileges;
Objects: Database object;
Object attributes: Object privileges, any attribute].

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

A user may access an object if:

a) the user is the owner of the object or has been granted specific object privileges;

b) the user has been granted specific system or schema privileges allowing access to the object;

c) the user is a member of a role that has been granted specific object and/or system or schema privileges;

d) the object is accessible by 'PUBLIC'].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

Application Note: A database object is an object in the database that may be manipulated with SQL. These include tables, cases, files, and views. An attribute is a property or detail associated with an object. 'Any attribute' refers to any property or detail associated with a database object.

Application Note: 'PUBLIC' is a special role granted to all users.

6.2.1.3 Subset residual information protection – FDP_RIP.1

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* the following objects: [*table, row*].

6.3 Identification and authentication – FIA

6.3.1 User attribute definition – FIA_ATD

6.3.1.1 User attribute definition – FIA_ATD.1

Hierarchical to: No other components.
Dependencies: No dependencies.

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

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

b) **Security-relevant database roles; and**

c) [*object privileges, schema privileges, system privileges, any attribute*].

Application Note: The intent of this requirement, as described in the DBMS cPP, is to specify the TOE security attributes that the TOE utilizes to determine access. However, it should be noted that the object privileges, system and schema privileges and attributes, although used in the access control decision, are not specifically associated with individual users.

Application Note: An attribute is a property or detail associated with an object. 'Any attribute' refers to any property or detail associated with a database object.

6.3.2 User authentication – FIA_UAU

6.3.2.1 User authentication before any action – FIA_UAU.2

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.3.3 User identification – FIA_UID

6.3.3.1 User identification before any action – FIA_UID.2

Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No other components

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.3.4 User-subject binding – FIA_USB

6.3.4.1 Enhanced user-subject binding – FIA_USB.2_EXT

Hierarchical to: FIA_USB.1 User-subject binding
Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.2.1_EXT The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*Database user identifier*, *roles, privileges*].

FIA_USB.2.2_EXT The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [*an authorized administrator may allow a proxy user to perform database operations on behalf on another user*].

FIA_USB.2.3_EXT The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [

a) granting and revoking of directly assigned privileges are effective immediately;

b) granting and revoking of indirectly assigned privileges are effective at the next log in].

FIA_USB.2.4_EXT The TSF shall enforce the following rules for the assignment of subject security attributes not derived from user security attributes when a subject is created: [*the proxy may be limited to the privileges of a particular role when acting on behalf of another user*].

6.4 Security management – FMT

6.4.1 Management of security attributes – FMT_MSA

6.4.1.1 Management of security attributes - FMT_MSA.1(1) (Users)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MSA.1.1(1) The TSF shall enforce the [*Discretionary Access Control Policy*] to restrict the ability to [*manage*] the security attributes associated with the *[users]* to [*authorised administrators*].

6.4.1.2 Management of security attributes - FMT_MSA.1(2) (Objects)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MSA.1.1(2) The TSF shall enforce the [*Discretionary Access Control Policy*] to restrict the ability to [*manage*] the security attributes associated with the [*objects*] to [*authorised administrators, authorized users*].

6.4.1.3 Static attribute initialization - FMT_MSA.3

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

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

FMT_MSA.3.2 The TSF shall allow ~~the~~ [no user] to specify alternative initial values to override the default values when an object or information is created.

6.4.2 Management of TSF data – FMT_MTD

6.4.2.1 Management of TSF data - FMT_MTD.1

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MTD.1.1 The TSF shall restrict the ability to [*include or exclude*] the [*auditable events*] to [*authorized administrators*].

6.4.3 Revocation - FMT_REV

6.4.3.1 Revocation - FMT_REV.1(1) (Users)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_REV.1.1(1) The TSF shall restrict the ability to revoke [*system and schema privileges, roles*] associated with the [users] under the control of the TSF to [*the authorised administrator*].

FMT_REV.1.2(1) The TSF shall enforce the rules [

a) granting and revoking of directly assigned privileges are effective immediately; and

b) granting and revoking of indirectly assigned privileges are effective at the next log in].

6.4.3.2 Revocation - FMT_REV.1(2) (Objects)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_REV.1.1(2) The TSF shall restrict the ability to revoke [*object privileges*] associated with the [objects] under the control of the TSF to [*the authorized administrator, authorized users*].

FMT_REV.1.2(2) The TSF shall enforce the rules [

a) authorized administrators and object owners may revoke object privileges; and

b) object owners may grant other users' privileges to grant and revoke object privileges].

6.4.4 Specification of management functions - FMT_SMF

6.4.4.1 Specification of management functions - FMT_SMF.1

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following **security** management functions:

[

- Database configuration
- User and role management

[

- No other security management functions[1]

]

[

- *management of the events to be audited;*
- *granting or revoking of system privileges;*
- *granting or revoking of schema privileges;*
- *granting or revoking of object privileges;*

[1] The security management functions listed in the SFR selection in the cPP are replaced by the security management functions listed in the assignment.

- *changes to user accounts (including authentication) and roles;*
- *configuration of Active Data Guard replication options;*
- *configuration of the maximum number of concurrent sessions for an individual user;*
- *configuration of separate domains for pluggable databases within a container database; and*
- *creation of dedicated services for a PDB*

]

].

6.4.5 Security roles – FMT_SMR

6.4.5.1 Security roles – FMT_SMR.1

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*authorized administrator, authorized users, and [database local user, database common user, and other roles defined by authorized administrators*]].

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

6.5 Protection of the TSF – FPT

6.5.1 Internal TOE TSF data replication consistency – FPT_TRC

6.5.1.1 Internal TSF consistency – FPT_TRC.1

Hierarchical to: No other components.

Dependencies: FPT_ITT.1 Basic internal TSF data transfer protection

FPT_TRC.1.1 The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2 When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [*queries*].

6.6 TOE access – FTA

6.6.1 Limitation on multiple concurrent sessions – FTA_MCS

6.6.1.1 Basic limitation on multiple concurrent sessions – FTA_MCS.1

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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 [*an administrator configurable number of*] sessions per user.

6.6.2 Configurable session limiting mechanisms - FTA_MCS_EXT

6.6.2.1 Configurable session limiting mechanisms - FTA_MCS_EXT.1

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_MCS_EXT.1.1: The TSF shall restrict the maximum number of concurrent sessions based on [User session locking as defined by FTA_MCS.1].

FTA_MCS_EXT.1.2: The TSF shall provide the capability for an authorized administrator to configure the selected enforcement mechanisms.

6.6.3 TOE access information – FTA_TAH

6.6.3.1 TOE access information – FTA_TAH.2_EXT

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TAH.2.1_EXT Upon a session establishment attempt, the TSF shall store

a) the date and time of the session establishment attempt of the user.

b) the incremental count of successive unsuccessful session establishment attempt(s).

FTA_TAH.2.2_EXT Upon successful session establishment, the TSF shall allow the date and time of

a) the previous last successful session establishment, and

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

to be retrieved by the user.

6.6.4 TOE session establishment – FTA_TSE

6.6.4.1 TOE session establishment – FTA_TSE.1

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [*attributes that can be set explicitly by authorized administrator(s), including user identity, and [[no additional attributes]]*].

6.7 Security Assurance Requirements

The security assurance requirements according to Table 14 have been chosen. They comprise EAL2 augmented by ALC_FLR.3.

Assurance Class	Assurance Component
Development - ADV	Security architecture description (ADV_ARC.1)
	Security-enforcing functional specification (ADV_FSP.2)
	Basic design (ADV_TDS.1)
Guidance documents - AGD	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life-cycle support - ALC	Use of a CM system (ALC_CMC.2)
	Parts of the TOE CM coverage (ALC_CMS.2)
	Delivery procedures (ALC_DEL.1)
	Systematic flaw remediation (ALC_FLR.3)
Security Target - ASE	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)
	Security objectives (ASE_OBJ.2)
	Derived security requirements (ASE_REQ.2)
	Security problem definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Tests - ATE	Evidence of coverage (ATE_COV.1)
	Functional testing (ATE_FUN.1)
	Independent testing – sample (ATE_IND.2)
Vulnerability assessment - AVA	Vulnerability analysis (AVA_VAN.2)

Table 14, Security Assurance Requirements

The Supporting Document [SD] contains evaluation activities that refine the evaluation activities for all assurance classes given in [CEM].

6.8 Security Requirements Rationale

6.8.1 Security Functional Requirements Dependencies

Functional Requirement	Direct explicit dependencies	Dependencies satisfied by
FAU_GEN.1	FPT_STM.1	This requirement is satisfied by the assumption on the IT environment, given in A.SUPPORT.
FAU_GEN.2	FAU_GEN.1	This requirement is satisfied by FAU_GEN.1.

Functional Requirement	Direct explicit dependencies	Dependencies satisfied by
	FIA_UID.1	This requirement is satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1.
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	This requirement is satisfied by FAU_GEN.1. This requirement is satisfied by FMT_MTD.1.
FDP_ACC.1	FDP_ACF.1	This requirement is satisfied by FDP_ACF.1.
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	This requirement is satisfied by FDP_ACC.1. This requirement is satisfied by FMT_MSA.3.
FDP_RIP.1	None	N/A
FIA_ATD.1	None	N/A
FIA_UAU.2	FIA_UID.1	This requirement is satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1.
FIA_UID.2	None	N/A
FIA_USB.2_EXT	FIA_ATD.1	This requirement is satisfied by FIA_ATD.1.
FMT_MSA.1(1)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	This requirement is satisfied by FDP_ACC.1. This requirement is satisfied by FMT_SMF.1. This requirement is satisfied by FMT_SMR.1.
FMT_MSA.1(2)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	This requirement is satisfied by FDP_ACC.1. This requirement is satisfied by FMT_SMF.1. This requirement is satisfied by FMT_SMR.1.
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	This requirement is satisfied by FMT_MSA.1(1). This requirement is satisfied by FMT_MSA.1(2). This requirement is satisfied by FMT_SMR.1.
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	This requirement is satisfied by FMT_SMF.1. This requirement is satisfied by FMT_SMR.1.
FMT_REV.1(1)	FMT_SMR.1	This requirement is satisfied by FMT_SMR.1.
FMT_REV.1(2)	FMT_SMR.1	This requirement is satisfied by FMT_SMR.1.
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	This requirement is satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1.
FPT_TRC.1	FPT_ITT.1	The dependency is satisfied through the environmental assumption, A.CONNECT, that assures the confidentiality and integrity of the transmitted data.
FTA_MCS.1	FIA_UID.1	This requirement is satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1.
FTA_MCS_EXT.1	None	N/A
FTA_TAH.2_EXT	None	N/A
FTA_TSE.1	None	N/A

Table 15, SFR dependencies

According to Table 15 all SFR dependencies are met.

6.8.2 Security Assurance Dependencies Analysis

The chosen evaluation assurance level EAL2 augmented by ALC_FLR.3. Since all dependencies are met internally by the EAL package only the augmented assurance components dependencies are analysed.

Functional Requirement	Direct explicit dependencies	Dependencies satisfied by
ALC_FLR.3	None	N/A

Table 16, SAR dependencies

According to Table 16 all SAR dependencies are met.

6.8.3 Security Functional Requirements Coverage

	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.DISCRETIONARY_ACCESS	O.I&A	O.MANAGE	O.RESIDUAL_INFORMATION	O.TOE_ACCESS
FAU_GEN.1		X					
FAU_GEN.2		X					
FAU_SEL.1		X					
FDP_ACC.1			X				X
FDP_ACF.1			X				X
FDP_RIP.1						X	
FIA_ATD.1				X			X
FIA_UAU.2				X			
FIA_UID.2				X			
FIA_USB.2_EXT				X			
FMT_MSA.1(1)					X		
FMT_MSA.1(2)					X		
FMT_MSA.3					X		
FMT_MTD.1					X		
FMT_REV.1(1)					X		
FMT_REV.1(2)					X		
FMT_SMF.1					X		
FMT_SMR.1	X				X		
FPT_TRC.1							X
FTA_MCS.1							X
FTA_MCS_EXT.1							X
FTA_TAH.2_EXT							X
FTA_TSE.1							X

Table 17, Security Functional Requirements Coverage

6.8.4 Security Functional Requirements Sufficiency

Objective	SFR	Rationale
O.ADMIN_ROLE The TOE shall provide roles that allow only authorized users to have access to administrative privileges that are specific to the role.	FMT_SMR.1	The TOE will establish, at least, an authorized administrator role. The authorized administrator will be given privileges to perform certain tasks that other users will not be able to perform. These privileges include, but are not limited to, access to audit information and security functions. For multitenant purposes, two classes of users, local users and common users, are defined. These user types are used to restrict administrative privileges. Additional roles may also be specified by authorized administrators.
O.AUDIT_GENERATION The TOE shall provide the capability to detect and create/generate records of security relevant events associated with users.	FAU_GEN.1 FAU_GEN.2 FAU_SEL.1	FAU_GEN.1 defines the set of events that the TOE is capable of recording. This requirement ensures that the administrator has the ability to audit any security relevant events that takes place in the TOE. This requirement also defines the information that is contained in the audit record for each auditable event. FAU_GEN.2 ensures that the audit records associate a user and any associated group identity with the auditable event. FAU_SEL.1 allows the administrator to configure which auditable events will be recorded in the audit trail, based on specified attributes.
O.DISCRETIONARY_ACCESS The TSF shall control access of subjects and/or users to named resources based on identity of the object, subject, or user. The TSF shall allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.	FDP_ACC.1 FDP_ACF.1	The TSF controls access to resources based on the subject's identity, role and/or system privileges and/or the object's security attributes.
O.I&A The TOE shall ensure that users are authenticated before the TOE processes any actions that require authentication.	FIA_ATD.1 FIA_UAU.2 FIA_UID.2 FIA_USB.2_EXT	FIA_UID.2 and FIA_UAU.2 ensure that only authorized users gain access to the TOE and its resources following identification and authentication. FIA_ATD.1 ensures that the security attributes used to determine access are defined and available to support the access control decisions.

Objective	SFR	Rationale
		FIA_USB.2_EXT ensures enforcement of the rules governing subjects acting on behalf of authorized users.
O.MANAGE The TSF shall provide all the functions and facilities necessary to manage TOE security mechanisms, and shall restrict such management actions to authorized users.	FMT_MSA.1(1) FMT_MSA.1(2) FMT_MSA.3 FMT_MTD.1 FMT_REV.1(1) FMT_REV.1(2) FMT_SMF.1 FMT_SMR.1	FMT_MSA.1(1) ensures that the ability to perform operations on security attributes associated with users is restricted to authorized administrators. FMT_MSA.1(2) ensures that the ability to perform operations on security attributes associated with objects is restricted to authorized administrators and authorized users. FMT_MSA.3 ensures that default values used for security attributes are restrictive. FMT_MTD.1 ensures that the ability to include or exclude auditable events is restricted to authorized administrators. FMT_REV.1(1) restricts the ability to revoke user attributes to the authorized administrator. FMT_REV.1(2) restricts the ability to revoke object attributes to the authorized administrator and authorized users. FMT_SMF.1 identifies the management functions that are available to the authorized administrator. FMT_SMR.1 defines the specific security roles to be supported.
O.RESIDUAL_INFORMATION The TOE shall ensure that any information contained in a protected resource within its control is not inappropriately disclosed when the resource is reallocated.	FDP_RIP.1	FDP_RIP.1 ensures that the contents of resources are not available upon reallocation of the resource.
O.TOE_ACCESS The TOE shall provide functionality that controls a user's logical access to user data and to the TSF.	FDP_ACC.1 FDP_ACF.1 FIA_ATD.1 FTA_MCS.1 FTA_MCS_EXT.1 FTA_TSE.1 FTA_TAH.2_EXT FPT_TRC.1	FDP_ACC.1 and FDP_ACF.1 ensure that access between subjects and objects is controlled using security attributes. FIA_ATD.1 defines the security attributes for individual users. FTA_MCS.1 and FTA_MCS_EXT.1 ensures that users are restricted to no more than a specified number of concurrent sessions. FTA_TSE.1 allows the TOE to restrict access to the TOE based on specified criteria. FTA_TAH.2_EXT The TOE will store and retrieve information about previous unauthorized login attempts and the number of times the login was

Objective	SFR	Rationale
		attempted every time the user logs into their account. The TOE will also store the last successful authorized login. This information will include the date, time, method, and location of the attempts. Access to this data is controlled and restricted such that a user may only access his or her own data. FPT_TRC.1 ensures replicated TSF data that specifies attributes for access control must be consistent across distributed components of the TOE. The requirement is to maintain consistency of replicated TSF data and associated access controls.

Table 18, Security Functional Requirements Sufficiency

6.8.5 Justification of the Chosen Evaluation Assurance Level

The collaborative Protection Profile (cPP) was developed for use by commercial DBMS security software developers. Since the cPP applies to commercial DBMS products that are used internationally the EAL2 assurance package was selected by the cPP writers to meet the maximum level of assurance that is recognized internationally through the Common Criteria Recognition Arrangement (CCRA).

Flaw Remediation is the only requirement not included in any EAL level because it does not add any assurance to the current system, but to subsequent releases. A systematic flaw remediation procedure is however considered necessary for every DBMS vendor who supports enterprise security needs in both, private and public sectors. Therefore, ALC_FLR.3 was selected to augment EAL2.

7 TOE Summary Specification

This section presents information to how the TOE meets the functional requirements described in previous sections of this ST.

Each of the security requirements and the associated descriptions correspond to security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements. Table 19 lists the security functions and their associated SFRs.

	Security Audit	User Data Protection	Identification and Authentication	Security Management	Protection of the TSF	TOE Access
FAU_GEN.1	**X**					
FAU_GEN.2	**X**					
FAU_SEL.1	**X**					
FDP_ACC.1		**X**				
FDP_ACF.1		**X**				
FDP_RIP.1		**X**				
FIA_ATD.1			**X**			
FIA_UAU.2			**X**			
FIA_UID.2			**X**			
FIA_USB.2_EXT			**X**			
FMT_MSA.1(1)				**X**		
FMT_MSA.1(2)				**X**		
FMT_MSA.3				**X**		
FMT_MTD.1				**X**		
FMT_REV.1(1)				**X**		
FMT_REV.1(2)				**X**		
FMT_SMF.1				**X**		
FMT_SMR.1				**X**		
FPT_TRC.1					**X**	
FTA_MCS.1						**X**
FTA_MCS_EXT.1						**X**
FTA_TAH.2_EXT						**X**
FTA_TSE.1						**X**

Table 19, TOE Security Functions

7.1 Security Audit

Oracle AI Database 26ai supports the auditing mechanism called unified auditing. Unified auditing will be used to meet the auditing requirements of the DBMS cPP.

The AUDIT statement is used to track the issuance of specific SQL statements, or all SQL statements authorized by a particular system privilege. It may also be used to track operations on a specific schema object. The UNIFIED_AUDIT_TRAIL table captures all the Unified Audit records while the database is open. Entries for start-up and shutdown events are sent to the operating system for logging.

Audit policies may be created and managed (using the CREATE AUDIT POLICY, ALTER AUDIT POLICY, and DROP AUDIT POLICY SQL statements) to determine exactly which events are audited, based on numerous criteria including use of particular roles or privileges. Each record includes the date and time of the event (EVENT_TIMESTAMP), type of event (ACTION_NAME), subject identity (DBUSERNAME, if applicable), and outcome (RETURN_CODE).

The policies required to capture the auditable events detailed in Column 2 of Table 13, Auditable events, are generally established through Unified Audit policies. However, the following details should be noted:

a. For the auditing requirements of FPT_TRC.1, restoring consistency, the actions are recorded on the primary database. The secondary database is an exact replica of the primary and therefore does not include platform specific audit records; and

b. For the auditing requirements for FTA_MCS.1, rejection of a new session based on the limitation of multiple concurrent sessions, the audit record appears as a failed login. However, the error code indicates the reason for failure (SESSION_PER_USER).

The following attributes are used to select the set of events to be audited from the set of all auditable events:

a) user identity;
b) object identity;
c) success of auditable security events; and
d) failure of auditable security events.

7.2 User Data Protection

FDP_ACC.1 and FDP_ACF.1 are used to describe how database users are granted access to database objects. Database objects are defined as any object in the database that may be manipulated with SQL. This includes, but is not limited to tables, rows, columns, cases, files, and views.

Access may be granted in one of several ways:

a) An object privilege is a system-defined privilege that controls access to a specific object. A database user has access to an object if the user is the owner of the object. In this case, the user has object privileges for the object. Object privileges may be granted to other users, as well. These privileges may be limited to certain operations. For example, the owner may be able to perform any operation (e.g. read, write, etc.), but another user may have read only access to the object;

b) A system or schema privilege may be granted to or revoked from a user by an administrator. These privileges allow users to perform specific database operations. For example, a user with the CREATE ANY TABLE system privilege may create a table in any schema and GRANT SELECT ANY TABLE ON SCHEMA HR TO SCOTT; will grant SELECT ANY TABLE privilege to SCOTT only for the HR schema;

c) A role is a collection of privileges and other roles. Some system-defined roles exist, but most are created by administrators to provide the least privilege required to perform the assigned tasks. Roles group together privileges and other roles, which facilitates the granting of multiple privileges and roles to users. Roles may be granted object, schema, and system privileges in much the same way that users may be granted these privileges. A user in a role would have the ability to perform actions permitted by the privileges;

d) An object privilege may grant access to users in the 'PUBLIC' role. The PUBLIC role is a special role automatically provided to every database account. By default, it has no privileges assigned to it, but it is granted access to many objects. The PUBLIC role may not be granted or revoked because the user account will always assume this role. Because all database user accounts assume the PUBLIC role, it does not appear in any list of roles.

Once a resource is allocated to a table, row or other database object, the previous content of that resource is overwritten and no longer available.

7.3 Identification and Authentication

To create a user, the administrator must provide a user account name and a password, and limitations on the resources available to the user. These limitations are in the form of defined tablespace and profile information. The tablespace assignment limits the number of resources available to the user and is measured in bytes. The profile associates the user with session limitations, such as the number of concurrent sessions allowed, and password parameters, such as the number of failed login attempts allowed before the account is locked, minimum password length, password complexity, and other password policies.

Users are granted privileges, such as the right to run a particular type of SQL statement, or the right to access an object that belongs to another user. Roles are created to group together privileges and other roles, making it easier to grant multiple privileges to a new user. A role must first be created by identifying the role, and then adding privileges. Once the role is defined, it may be granted to a user.

In addition to granting object, schema, and system privileges to users through roles, these privileges may also be granted to users individually.

Users may be granted access to database objects based on any attribute. When configured, the policy appends a WHERE clause to queries to control access at the row and column level. This could be used to allow users to query a human resources table, but only see their own information, or only certain columns associated with the employees who report to these users. This policy (and therefore, this attribute) is not directly associated with the database user's account. Please note that these users must also have object or system privileges to access the database objects. Attributes may be used to provide a more fine-grained access control to data within accessible objects.

Oracle AI Database 26ai ensures that users are identified and authenticated prior to being allowed access to database objects or resources. Although several authentication mechanisms

are supported, only local username and password authentication is examined for the purposes of this evaluation.

One database user may act with the privileges of another as a proxy user. To enable this, the user must be granted permission to access the database through a proxy. This grant operation may specify which roles (and therefore which privileges) are enabled for this access. In this way, the proxy access may be limited to a specific set of required privileges, rather than all of the primary user's privileges. This is typically used in cases where the proxy user is an application server or middle tier entity.

When a directly assigned privilege is granted or revoked, this takes effect immediately. This includes granting or revoking object, schema, or system privileges, or granting or revoking object, schema, or system privileges from a role. When an indirectly assigned privilege is granted or revoked, this is effective at the next login. This includes adding or removing a role from a user account.

The security attributes belonging to individual users are:

a) Database user identifier;
b) Security-relevant database roles; and
c) Object privileges, schema privileges, system privileges, any attribute.

Where roles are described above and 'any attribute' refers to any property or detail associated with a database object.

Database user identifier, roles, and privileges are associated with subjects acting on the behalf of a user.

An authorized administrator may allow a proxy user to perform database operations on behalf on another user. The proxy may be limited to the privileges of a particular role when acting on behalf of another user.

Granting and revoking of directly assigned privileges are effective immediately while granting and revoking of indirectly assigned privileges are effective at the next log in.

7.4 Security Management

An audit policy determines which events are to be audited. The privileges required to specify this policy are only available to authorized administrators.

The access control decision for the Discretionary Access Control Policy is made based on object privileges, schema privileges, system privileges, roles and any attribute. All of these attributes may be managed by authorized administrators. Object privileges and attributes may also be managed by their owners, or users to whom the owner has granted that privilege. In this case, the owner or delegated user is considered to be an authorized administrator of the object or attribute. The default values for these attributes are restrictive. System privileges, schema privileges, object privileges and roles must be specifically granted to users. Attribute values do not permit access until a policy granting that access has been created by an authorized administrator.

Only authorized administrators may revoke system privileges, schema privileges, and roles. Revocation of directly assigned system or schema privileges (i.e. system privileges granted directly to a user or a role) takes effect immediately. Revocation of a role from a user account is effective at the next login.

Authorized administrators and object owners may revoke object privileges. The ability to grant and revoke object privileges may also be granted to other users by an authorized administrator, or the object owner.

Authorized administrators and schema owners may revoke schema privileges. The ability to grant and revoke schema privileges may also be granted to other users by an authorized administrator, or the schema owner.

The TOE is managed by submitting SQL statements to the database using the SQL *Plus command line interface. The commands allow authorized administrators to perform all of the security management functionality required to manage the claimed security features of the TOE including:

a) management of the events to be audited;

b) changes to the system privileges;

c) changes to the schema privileges;

d) changes to the object privileges;

e) changes to user accounts (including changes to authentication options) and roles;

f) configuration of Data Guard options in support of the replication requirements;

g) configuration of the maximum number of concurrent sessions for an individual user;

h) configuration of separate domains for pluggable databases within a container database; and

i) creation of dedicated services for a Pluggable Database.

Each database requires at least one user in the database administrator role. (This role is described as ‘authorized administrator’ in the SFRs.) Other administrative roles may be created by authorized administrators with the unique set of system and object privileges required to perform assigned tasks. Database users make use of the database, but do not typically have administrative system privileges.

7.5 Protection of the TSF

The TOE provides replication of data using the Data Guard feature. Primary database transactions generate redo records. A redo record is made up of a group of change vectors, each of which is a description of a change made to a single block in the database. For example, if a value is changed in a table, a redo record containing change vectors that describe changes to the data segment block for the table, the undo segment data block and the transaction table of the undo segments is generated. Data Guard works by shipping the redo to the replicated database and then applying that redo.

Redo records contain all the information needed to reconstruct changes made to the database. During media recovery, the database will read change vectors in the redo records and apply the changes to the relevant blocks. When configured to use the Synchronous transport method (also called the "zero data loss" method), the commit operation will not be confirmed until it is written to both the local and the remote database. If the connection between the databases is lost, updates to the primary database are halted until the secondary database is reconnected, thereby assuring consistency of the replicated data.

7.6 TOE Access

The TSF may restrict the maximum number of concurrent sessions for a user. This is configured using the SESSIONS_PER_USER option in the resource parameters of a profile assigned to a user. Although the default value is unlimited, in the evaluated configuration, an authorized administrator must select a finite number for this limit.

Upon user login, the date and time of the successful or unsuccessful login attempt is saved in the audit records. The audit records also maintain a count of successive unsuccessful login attempts. In order to maintain the date and time of the last successful login, the last unsuccessful login attempt and the number of unsuccessful attempts since the previous last successful login, and make that data accessible to the user, a custom query must be used. This custom SQL script is run to retrieve the required information, which may then be viewed by the user.

The TOE is able to deny session establishment based on user identity by dropping the user account.

Appendix A – Abbreviations and Acronyms

Acronym	Definition
CC	Common Criteria
CCRA	Common Criteria Recognition Agreement
CDB	Container Database
CEM	Common Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
CM	Configuration Management
CPU	Critical Patch Update
DAC	Discretionary Access Control
DBMS	Database Management System
DBMS PP	Base Protection Profile for Database Management Systems
DDL	Data Definition Language
DML	Data Manipulation Language
EAL	Evaluation Assurance Level
I&A	Identification and Authentication

Acronym	Definition
IP	Internet Protocol
IT	Information Technology
MAC	Mandatory Access Control
OLS	Oracle Label Security
OSP	Organizational Security Policy
PDB	Pluggable Database
PL/SQL	Procedural Language Extension to Structured Query Language
PP	Protection Profile
RAC	Real Application Clusters
RDBMS	Relational Database Management System
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
WG/TC	Working Group/Technical Community

Table 20, Abbreviations and acronyms

Appendix B – Terms and Definitions

Term	Description
Access	Interaction between an entity and an object that results in the flow or modification of data.
Access Control	Security service that controls the use of resources[2] and the disclosure and modification of data[3].
Accountability	Property that allows activities in an IT system to be traced to the entity responsible for the activity.
Administrator	A user who has been specifically granted the authority to manage some portion or the entire TOE and whose actions may affect the TOE security policy. Administrators may possess special privileges that provide capabilities to override portions of the TOE security policy.
Assurance	A measure of confidence that the security features of an IT system are sufficient to enforce its security policy.
Attack	An intentional act attempting to violate the security policy of an IT system.
Attribute	An attribute is a property or detail associated with an object.
Authentication	Security measure that verifies a claimed identity.
Authentication data	Information used to verify a claimed identity.
Authorization	Permission, granted by an entity authorized to do so, to perform functions and access data.
Authorized Administrator	The authorized person in contact with the Target of Evaluation who is responsible for maintaining its operational capability.
Authorized user	An authenticated user who may, in accordance with the TOE security policy, perform an operation.
Availability	Timely[4], reliable access to IT resources.
Compromise	Violation of a security policy.
Confidentiality	A security policy pertaining to the disclosure of data.
Configuration data	Data this is used in configuring the TOE.

[2] Hardware and software

[3] Stored or communicated

[4] According to a defined metric

Term	Description
Conformant Product	A Target of Evaluation that satisfied all the functional security requirements and satisfies all the TOE security assurance requirements.
Database Management System (DBMS)	A suite of programs that typically manage large structured sets of persistent data, offering ad hoc query facilities to many users. They are widely used in business applications.
Discretionary Access Control (DAC)	A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. Those controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.
Enclave	A collection of entities under the control of a single authority and having a homogeneous security policy. They may be logical, or may be based on physical location and proximity.
Entity	A subject, object, user or another IT device, which interacts with TOE objects, data, or resources.
Executable code within the TSF	The software that makes up the TSF which is in a form that can be run by the computer.
External IT entity	Any trusted Information Technology (IT) product or system, outside of the TOE, which may, in accordance with the TOE security policy, perform an operation.
Identity	A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Integrity	A security policy pertaining to the corruption of data and TSF mechanisms.
Named Object	An object that exhibits all of the following characteristics: • The object may be used to transfer information between subjects of differing user and/or group identities within the TSF. • Subjects in the TOE must be able to require a specific instance of the object. • The name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with different user and/or group identities to require the same instance of the object.
Object	An entity within the TOE scope of control that contains or receives information and upon which subjects perform operations.
Operating Environment	The total environment in which a TOE operates. It includes the physical facility and any physical, procedural, administrative and personnel controls.
Public Object	An object for which the TSF unconditionally permits all entities “read” access. Only the TSF or authorized administrators may create, delete, or modify the public objects.
Resource	The term ‘resources’ is used to describe data resources such as database objects.

Term	Description
Secure State	Condition in which all TOE security policies are enforced.
Security attributes	TSF data associated with subjects, objects, and users that are used for the enforcement of the TOE security policy.
Security level	The combination of a hierarchical classification and a set of non-hierarchical categories that represent the sensitivity of the information.
Sensitive information	Information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something.
Subject	An entity within the TOE scope of control that causes operation to be performed.
Threat	Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.
TOE resources	Anything useable or consumable in the TOE.
Unauthorized user	A user who may obtain access only to system provided public objects if any exist.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Vulnerability	A weakness that can be exploited to violate the TOE security policy.

Table 21, Terms and definitions

Appendix C - Referenced Documents

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

[4] Common Methodology for Information Technology Security Evaluation, CCMB-2017-04-004, Version 3.1, Revision 5, April 2017

[5] collaborative Protection Profile for Database Management Systems, Version 1.3, 13 March 2023

[6] Supporting Document Mandatory Technical Document Evaluation Activities for the collaborative Protection Profile for Database Management Systems, Version 1.1, 15 March 2023