DBMS cPP Version 2.0 Tracked Changes from v1.3

Field	Value
Baseline	DBMS cPP v1.3 official PDF (13 March 2023)
Compared to	DBMS cPP v2.0 Public Review Draft 1 PDF (26 June 2026)
Generated	2026-06-26 16:43 UTC

This comparison is generated from normalized text extracted from the posted official PDF and the review draft PDF.

```
--- DBMS cPP v1.3 official PDF (13 March 2023)
+++ DBMS cPP v2.0 Public Review Draft 1 PDF (26 June 2026)
@@ -1,694 +1,577 @@
 collaborative Protection Profile for
 Database Management Systems
-13 March 2023
-Version 1.3
+26 June 2026
+Version 2.0
 Acknowledgements
-This collaborative Protection Profile (cPP) was developed by the Database
-Management System international Technical Community with representatives from
-industry, Government agencies, Common Criteria Test Laboratories. The
-organizations that contributed to the development of this cPP include:
-Industry
+This collaborative Protection Profile (cPP) was developed by the Database Management
System
+international Technical Community with representatives from industry, Government
agencies,
+Common Criteria Test Laboratories. The organizations that contributed to the development
of this
+cPP include:
+INDUSTRY
 IBM
 Microsoft
 Oracle Corp.
-Common Criteria Test Laboratories
+COMMON CRITERIA TEST LABORATORIES
 atsec information security
 Intertek EWA-Canada and Intertek Acumen
 TÜViT
```

```
 Teron Labs
 Combitech
-Government Agencies
+GOVERNMENT AGENCIES
 FMV/CSEC - Swedish Certification Body for IT Security
 BSI - Bundesamt für Sicherheit in der Informationstechnik
 JISEC - Japan IT Security Evaluation and Certification Scheme
 Details of how to contact the DBMS iTC are found on the Common Criteria Portal at:
 https://www.commoncriteriaportal.org/communities/index.cfm
-1. Preface
-1.1 Objectives of Document
-This document presents the Common Criteria (CC) collaborative Protection Profile
-(cPP) to express the security functional requirements (SFRs) and security assurance
-requirements (SARs) for a Database Management System. The Evaluation Activities
-that specify the actions the evaluator performs to determine if a product satisfies the
-SFRs captured within this cPP are described in the associated Supporting Document.
-1.2 Scope of Document
-The scope of the cPP within the development and evaluation process is described in
-the Common Criteria for Information Technology Security Evaluation [CC1]. In
-particular, a cPP defines the IT security requirements of a generic type of TOE and
-specifies the functional and assurance security measures to be offered by that TOE
-to meet stated requirements [[CC1], section C.1].
-1.3 Intended Readership
-The target audiences of this cPP are DBMS developers, CC consumers, system
-integrators, CC evaluators and CCRA schemes.
-Although the cPPs and SDs may contain minor editorial errors, cPPs are recognized
-as living documents and the iTCs are dedicated to ongoing updates and revisions.
-Please report any issues to the DBMS iTC. Information on how to contact the DBMS
-iTC can be found on the Technical Communities information page.
-1.4 Related Documents
+Preface
+Objectives of Document
+This document presents the Common Criteria (CC) collaborative Protection Profile (cPP)
to express
+the security functional requirements (SFRs) and security assurance requirements (SARs)
for a
+Database Management System. The Evaluation Activities that specify the actions the
evaluator
+performs to determine if a product satisfies the SFRs captured within this cPP are
described in the
+associated Supporting Document.
+Scope of Document
+The scope of the cPP within the development and evaluation process is described in the
Common
+Criteria for Information Technology Security Evaluation [CC1]. In particular, a cPP
defines the IT
+security requirements of a generic type of TOE and specifies the functional and
assurance security
```

```
+measures to be offered by that TOE to meet stated requirements [[CC1], section C.1].
+Intended Readership
+The target audiences of this cPP are DBMS developers, CC consumers, system integrators,
CC
+evaluators and CCRA schemes.
+Although the cPPs and SDs may contain minor editorial errors, cPPs are recognized as
living
+documents and the iTCs are dedicated to ongoing updates and revisions. Please report any
issues to
+the DBMS iTC. Information on how to contact the DBMS iTC can be found on the Technical
+Communities information page.
+Related Documents
 The following documents are available from the CC Portal at
 https://www.commoncriteriaportal.org/
 Common Criteria
-[CC1] Common Criteria for Information Technology Security Evaluation,
-Part 1: Introduction and General Model,
-CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.
-https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
-[CC2] Common Criteria for Information Technology Security Evaluation,
-Part 2: Security Functional Components,
-CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.
-https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf
-[CC3] Common Criteria for Information Technology Security Evaluation,
-Part 3: Security Assurance Components,
-CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
-https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf
-[CEM] Common Methodology for Information Technology Security Evaluation,
-Evaluation Methodology,
-CCMB-2017-04-004, Version 3.1 Revision 5, April 2017
-https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf
+[CC1] Common Criteria for Information Technology
+Security Evaluation, Part 1: Introduction and
+general model, CCMB-2022-11-001, CC:2022
+Revision 1, November 2022.
+[CC2] Common Criteria for Information Technology
+Security Evaluation, Part 2: Security functional
+requirements, CCMB-2022-11-002, CC:2022
+Revision 1, November 2022.
+[CC3] Common Criteria for Information Technology
+Security Evaluation, Part 3: Security assurance
+requirements, CCMB-2022-11-003, CC:2022
+Revision 1, November 2022.
+[CC4] Common Criteria for Information Technology
+Security Evaluation, Part 4: Framework for the
+specification of evaluation methods and
+activities, CCMB-2022-11-004, CC:2022 Revision 1,
+November 2022.
```

```
+[CC5] Common Criteria for Information Technology
+Security Evaluation, Part 5: Pre-defined
+packages of security requirements, CCMB-2022-
+11-005, CC:2022 Revision 1, November 2022.
+[CCE] Common Criteria for Information Technology
+Security Evaluation, Errata and interpretation
+for CC:2022 (Release 1) and CEM:2022 (Release
+1), CCMB-002, Version 1.1, July 22, 2024.
+[CEM] Common Methodology for Information
+Technology Security Evaluation, Evaluation
+methodology, CCMB-2022-11-006, CEM:2022,
+Revision 1, November 2022.
 Documents related to this cPP
-[SD] Supporting Document Mandatory Technical Document Evaluation Activities for the
-collaborative Protection Profile for Database Management Systems, Version 1.1, 15
-March 2023
+[SD] Supporting Document Mandatory Technical
+Document Evaluation Activities for the
+collaborative Protection Profile for Database
+Management Systems, Version 2.0, 27 April 2026
 Other Documents
 [DBMSiTC] DBMS iTC Status
-https://www.commoncriteriaportal.org/files/communities/Status.DBMS.pdf
-[CCADD] CC and CEM Addenda: Exact Conformance, Selection-Based SFRs, Optional SFRs
-CCDB, Unique Identifier:013, Version 2.0, 2021-Sep-30
-1.5 Conventions
-Except for replacing United Kingdom spelling with American spelling, the notation,
-formatting, and conventions used in this cPP are consistent with version 3.1 of the
-CC. Selected presentation choices are discussed here to aid the cPP reader.
-The CC allows several operations to be performed on functional requirements;
-refinement, selection, assignment, and iteration are defined in clause 8 of Part 1 of
-the CC [CC1]. Each of these operations is used in this Protection Profile (PP).
-The refinement operation is used to add detail to a requirement, and thus further
-restricts a requirement. Refinement of security requirements is denoted by bold text
-or in the case of deletions, by crossed out bold text.
-The selection operation is used to select one or more options provided by the CC in
-stating a requirement. Selections that have been made by the PP authors are
-denoted by italicized text, selections to be filled in by the Security Target (ST)
author
-appear in square brackets with an indication that a selection is to be made,
-[selection:], and are not italicized.
-The assignment operation is used to assign a specific value to an unspecified
-parameter, such as the length of a password. Assignments that have been made by
-the cPP authors are denoted by showing the value in square brackets,
-[assignment_value], assignments to be filled in by the ST author appear in square
-brackets with an indication that an assignment is to be made [assignment:].
-Assignments within selections are denoted by showing the value in square brackets
-and italics [assignment_value].
```

```
-The iteration operation is used when a component is repeated with varying
-operations.
-Iteration is denoted by showing the iteration number in parenthesis following the
-component identifier, (iteration number).
-The CC paradigm also allows protection profile authors to create their own
-requirements. Such requirements are termed "extended requirements" and are
-permitted if the CC does not offer suitable requirements to meet the author's needs.
-Extended requirements must be identified and are required to use the CC
-class/family/component model in articulating the requirements. In this cPP, extended
-requirements will be indicated with the "_EXT" following the component name.
-Application Notes are provided to help the developer, either to clarify the intent of a
-requirement, identify implementation choices, or to define "pass-fail" criteria for a
-requirement. For those components where Application Notes are appropriate, the
-Application Notes will follow the requirement component. They are numbered and
-formatted thus:
+https://www.commoncriteriaportal.org/files/
+communities/Status.DBMS.pdf
+[TD_DBMS_B_001] Technical Decision TD_DBMS_B_001: Update to
+Role Definitions and Security Attribute
+Management for Consistency, published 29 July
+2025
+[TD_DBMS_B_002] Technical Decision TD_DBMS_B_002: Session
+Locking Mechanism Expansion, published 29
+July 2025
+Conventions
+Except for replacing United Kingdom spelling with American spelling, the notation,
formatting, and
+conventions used in this cPP are consistent with CC:2022. Selected presentation choices
are
+discussed here to aid the cPP reader.
+The CC allows several operations to be performed on functional requirements; refinement,
+selection, assignment, and iteration are defined in clause 8 of Part 1 of the CC [CC1].
Each of these
+operations is used in this Protection Profile (PP).
+The refinement operation is used to add detail to a requirement, and thus further
restricts a
+requirement. Refinement of security requirements is denoted by bold text or in the case
of
+deletions, by crossed out bold text.
+The selection operation is used to select one or more options provided by the CC in
stating a
+requirement. Selections are denoted in square brackets using the CC operation
designator,
+[selection: selection_value]. Selections to be filled in by the Security Target (ST)
author retain the
+available choices after the designator.
+The assignment operation is used to assign a specific value to an unspecified parameter,
such as
```

```
+the length of a password. Assignments are denoted in square brackets using the CC
operation
+designator, [assignment: assignment_value]. Assignments to be filled in by the Security
Target (ST)
+author retain placeholder text after the designator.
+The iteration operation is used when a component is repeated with varying operations.
+Iteration is denoted by showing the iteration number in parenthesis following the
component
+identifier, (iteration number).
+The CC paradigm also allows protection profile authors to create their own requirements.
Such
+requirements are termed "extended requirements" and are permitted if the CC does not
offer
+suitable requirements to meet the author's needs. Extended requirements must be
identified and
+are required to use the CC class/family/component model in articulating the
requirements. In this
+cPP, extended requirements will be indicated with the "_EXT" following the component
name.
+Application Notes are provided to help the developer, either to clarify the intent of a
requirement,
+identify implementation choices, or to define "pass-fail" criteria for a requirement.
For those
+components where Application Notes are appropriate, the Application Notes will follow
the
+requirement component. They are numbered and formatted thus:
 Application Note 1: This is an application note.
-1.6 Revision History
+Revision History
 Version Date Description
 0.01 14th February, 2019 Initial Release for iTC review
 0.02 8th March, 2019 After iTC workshop review
-0.03 16th June, 2019 Updated with the agreed SPD1 (V1.0) after Public Review
+0.03 16th June, 2019 Updated with the agreed SPD
+(V1.0) after Public Review
 0.04 28th October, 2019 Updates by iTC
-0.05 7 February 2020 Acceptance of changes, formatting changes
+Version Date Description
+0.05 7 February 2020 Acceptance of changes,
+formatting changes
 0.06 28 February 2020 Acceptance of changes
 1.0 16 June 2020 Initial Release
-1.1a 28 November 2022 Updated according to evaluator comments.
-1.1b 1 December 2022 Further comments from the evaluator
+1.1a 28 November 2022 Updated according to evaluator
+comments.
+1.1b 1 December 2022 Further comments from the
+evaluator
```

```
 1.2 13 December 2022 After iTC review
-1.3 13 March 2023 Updated according to certifier comments.
-1 Security Problem Definition
-Contents
-ACKNOWLEDGEMENTS
-1. PREFACE
-1.1 OBJECTIVES OF DOCUMENT
-1.2 SCOPE OF DOCUMENT
-1.3 INTENDED READERSHIP
-1.4 RELATED DOCUMENTS
-1.5 CONVENTIONS
-1.6 REVISION HISTORY
-2. CPP INTRODUCTION
-2.1 CPP REFERENCE IDENTIFICATION
-2.2 CPP OVERVIEW
-2.3 TOE OVERVIEW
-2.3.1 Database Management Systems overview
-2.3.2 Security Functionality Provided by the TOE
-2.3.3 TOE definition
-2.3.4 Limitations of Security Claims
-2.4 TOE OPERATIONAL ENVIRONMENT
-2.4.1 DBMS Architecture and Environmental Components
-2.4.2 TOE Administration
-3. CONFORMANCE CLAIMS
-3.1 CONFORMANCE WITH CC
-3.2 CONFORMANCE WITH CC PARTS 2 AND 3
-3.3 CONFORMANCE WITH PACKAGES
-3.4 CONFORMANCE WITH OTHER PROTECTION PROFILES
-3.5 CONFORMANCE STATEMENT
-3.6 PP-CONFIGURATION
-4. SECURITY PROBLEM DEFINITION
-4.1 INFORMAL DISCUSSION
-4.2 ASSETS AND THREAT AGENTS
-4.3 THREATS
-4.4 ORGANIZATIONAL SECURITY POLICIES
-4.5 ASSUMPTIONS
-5. SECURITY OBJECTIVES
-5.1 TOE SECURITY OBJECTIVES
-5.1.1 O.ADMIN_ROLE
-5.1.2 O.AUDIT_GENERATION
-5.1.3 O.DISCRETIONARY_ACCESS
-5.1.4 O.I&A
-5.1.5 O.MANAGE
-5.1.6 O.RESIDUAL_INFORMATION
-5.1.7 O.TOE_ACCESS
-5.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT
-5.2.1 OE.ADMIN
-5.2.2 OE.INFO_PROTECT
```

```
-5.2.3 OE.NO_GENERAL_ PURPOSE
-5.2.4 OE.PHYSICAL
-5.3 SECURITY OBJECTIVES FOR THE OPERATIONAL IT ENVIRONMENT
-5.3.1 OE.IT_I&A
-5.3.2 OE.IT_TRUSTED_SYSTEM
-6. SECURITY FUNCTIONAL REQUIREMENTS
-6.1 CLASS: SECURITY AUDIT (FAU)
-6.1.1 Audit Data Generation (FAU_GEN)
-FAU_GEN.1.1
-6.1.2 Security audit event selection (FAU_SEL)
-6.2 CLASS: USER DATA PROTECTION (FDP)
-6.2.1 Access control policy (FDP_ACC)
-6.2.2 Residual information protection (FDP_RIP)
-6.3 CLASS: IDENTIFICATION AND AUTHENTICATION (FIA)
-6.3.1 User authentication (FIA_UAU)
-6.3.2 User attribute definition (FIA_ATD)
-6.3.3 User identification (FIA_UID)
-6.4 CLASS: SECURITY MANAGEMENT (FMT)
-6.4.1 Management of security attributes (FMT_MSA)
-6.4.2 Management of TSF data (FMT_MTD)
-6.4.3 Revocation (FMT_REV)
-6.4.4 Specification of management functions (FMT_SMF)
-6.4.5 Security management roles (FMT_SMR)
-6.5 CLASS: TOE ACCESS (FTA)
-6.5.1 Limitation on multiple concurrent sessions (FTA_MCS)
-6.5.2 TOE session establishment (FTA_TSE)
-7. SECURITY ASSURANCE REQUIREMENTS
-7.1 CLASS ASE: SECURITY TARGET
-7.2 CLASS ADV: DEVELOPMENT
-7.3 CLASS AGD: GUIDANCE DOCUMENTATION
-7.4 CLASS ALC: LIFE-CYCLE SUPPORT
-7.5 CLASS ATE: TESTS
-7.6 CLASS AVA: VULNERABILITY ASSESSMENT
-A. OPTIONAL REQUIREMENTS
-A.1 CLASS: IDENTIFICATION AND AUTHENTICATION (FIA)
-A.1.1 Enhanced user-subject binding (FIA_USB_EXT)
-A.2 CLASS: PROTECTION OF THE TSF (FPT)
-A.2.1 Internal TOE TSF data replication consistency (FPT_TRC)
-A.3 CLASS: TOE ACCESS (FTA)
-A.3.1 TOE access information (FTA_TAH_EXT)
-B. EXTENDED COMPONENT DEFINITIONS
-B.1 CLASS: USER IDENTIFICATION AND AUTHENTICATION (FIA)
-B.1.1 Enhanced user-subject binding (FIA_USB_EXT)
-B.2 CLASS: TOE ACCESS (FTA)
-B.2.1 TOE access information (FTA_TAH_EXT)
-C. RATIONALES
-C.1 TOE SECURITY OBJECTIVES COVERAGE
-C.2 RATIONALE FOR TOE SECURITY OBJECTIVES
```

```
-C.3 RATIONALE FOR THE ENVIRONMENTAL SECURITY OBJECTIVES
-C.4 RATIONALE FOR TOE SECURITY FUNCTIONAL REQUIREMENTS
-C.5 SFR DEPENDENCIES ANALYSIS
-C.6 SAR DEPENDENCIES ANALYSIS
-C.7 RATIONALE FOR SATISFYING ALL SECURITY ASSURANCE REQUIREMENTS
-C.8 RATIONALE FOR EXTENDED SECURITY FUNCTIONAL REQUIREMENTS
-GLOSSARY
-TERMS AND DEFINITIONS
-ACRONYMS USED IN THIS CPP
-Figures / Tables
-Table 1: Threats Applicable to the TOE
-Table 2: Policies Applicable to the TOE
-Table 3: Assumptions Applicable to the TOE Environment
-Table 4: Auditable Events
-Table 5: Security Assurance Requirements
-Table 6: Coverage of Security Objectives for the TOE
-Table 7: Rationale for the TOE Security Objectives
-Table 8: Coverage of SPF Items for the TOE Environment Security Objectives
-Table 9: Rationale for Environmental Security Objectives
-Table 10: Rationale for TOE Security Functional Requirements
-Table 11: Rationale for Extended Security Functional Requirements
-2. cPP Introduction
-2.1 cPP Reference Identification
-cPP Reference: collaborative Protection Profile for Database Management
-Systems
-cPP Version: 1.3
-cPP Date: 13 March 2023
-2.2 cPP Overview
-This is a collaborative Protection Profile (cPP), a PP that meets the requirements for
-cPPs described in the Common Criteria Recognition Arrangement.
-Security Targets (STs) that claim conformance to this cPP shall claim exact
-conformance as defined in Addenda for Exact conformance the CC, [CCADD]
-The product type of the Target of Evaluation (TOE) described in this cPP is a
-database management system (DBMS). A database is an organized collection of
-data, generally stored and accessed electronically from a computer system. The
-database management system (DBMS) is the software that interacts with end users,
-applications, and the database itself to capture and analyze the data. The DBMS
-software additionally encompasses the core facilities provided to administer the
-database. A DBMS may be a single-user system, in which only one user may access
-the DBMS at a given time, or a multi-user system, in which many users may access
-the DBMS simultaneously.
-The DBMS will have the capability to limit DBMS access to authorized users, enforce
-Discretionary Access Controls (DAC) on objects under the control of the database
-management system based on user and optionally, group authorizations, and
-provide user accountability via audit of users' actions.
-This cPP specifies security requirements for a commercial-off-the-shelf (COTS)
-database management system (DBMS). The TOE type is a database management
-system.
```

```
-Security Targets (ST) derived from this cPP describe Targets of Evaluation (TOE)
-that are Database Management Systems.
-2.3 TOE Overview
-A TOE compliant with this cPP includes, but is not limited to, a DBMS server and can
-be evaluated as a software only application layered on an underlying system, i.e., an
-operating system (OS), hardware, network services, and/or custom software, and is
-usually embedded as a component of a larger system within an operational
-environment. This profile establishes the requirements necessary to achieve the
-security objectives of the Target of Evaluation (TOE) and its environment.
-Conformant TOEs provide access control based on user identity and, optionally,
-group membership, e.g., Discretionary Access Control (DAC), and generation of
-audit records for security relevant events. Authorized administrators of the TOE are
-trusted to not misuse the privileges assigned to them.
-2.3.1 Database Management Systems overview
-A DBMS is comprised of the DBMS server application that performs some or all of
-the following functions:
-a) Controlling TOE users' accesses to user data and TSF data;
-b) Indexing data values to their physical locations for quick retrievals based on a
-value or range of values;
-c) Executing pre-written programs (i.e., utilities) to perform common tasks like
-database backup, recovery, loading, and copying;
-d) Supporting mechanisms that enable concurrent database access (e.g., locks);
-e) Assisting recovery of user data and DBMS data (e.g., transaction log); and
-f) Tracking operations that users perform.
+1.3 13 March 2023 Updated according to certifier
+comments.
+1.4 25 April 2025 Updated after comments from
+BSI.
+1.5 27 April 2026 Incorporated TD_DBMS_B_001
+and TD_DBMS_B_002.
+2.0 27 April 2026 Updated conformance target to
+CC:2022.
+Chapter 1. cPP Introduction
+1.1. cPP Reference Identification
+cPP Reference: collaborative Protection Profile for Database Management Systems
+cPP Version: 2.0
+cPP Date: 27 April 2026
+1.2. cPP Overview
+This is a collaborative Protection Profile (cPP), a PP that meets the requirements for
cPPs described
+in the Common Criteria Recognition Arrangement.
+Security Targets (STs) that claim conformance to this cPP shall claim exact conformance
as defined
+in CC:2022 [CC1].
+The product type of the Target of Evaluation (TOE) described in this cPP is a database
management
+system (DBMS). A database is an organized collection of data, generally stored and
accessed
```

```
+electronically from a computer system. The database management system (DBMS) is the
software
+that interacts with end users, applications, and the database itself to capture and
analyze the data.
+The DBMS software additionally encompasses the core facilities provided to administer
the
+database. A DBMS may be a single-user system, in which only one user may access the DBMS
at a
+given time, or a multi-user system, in which many users may access the DBMS
simultaneously.
+The DBMS will have the capability to limit DBMS access to authorized users, enforce
Discretionary
+Access Controls (DAC) on objects under the control of the database management system
based on
+user and optionally, group authorizations, and provide user accountability via audit of
users'
+actions.
+This cPP specifies security requirements for a commercial-off-the-shelf (COTS) database
+management system (DBMS). The TOE type is a database management system.
+Security Targets (ST) derived from this cPP describe Targets of Evaluation (TOE) that
are Database
+Management Systems.
+1.3. TOE Overview
+A TOE compliant with this cPP includes, but is not limited to, a DBMS server and can be
evaluated
+as a software only application layered on an underlying system, i.e., an operating
system (OS),
+hardware, network services, and/or custom software, and is usually embedded as a
component of a
+larger system within an operational environment. This profile establishes the
requirements
+necessary to achieve the security objectives of the Target of Evaluation (TOE) and its
environment.
+Conformant TOEs provide access control based on user identity and, optionally, group
membership,
+e.g., Discretionary Access Control (DAC), and generation of audit data for security
relevant events.
+Authorized administrators of the TOE are trusted to not misuse the privileges assigned
to them.
+1.3.1. Database Management Systems overview
+A DBMS is comprised of the DBMS server application that performs some or all of the
following
+functions:
+ Controlling TOE users' accesses to user data and TSF data;
+ Indexing data values to their physical locations for quick retrievals based on a value
or range of
+values;
+ Executing pre-written programs (i.e., utilities) to perform common tasks like database
```

```
backup,
+recovery, loading, and copying;
+ Supporting mechanisms that enable concurrent database access (e.g., locks);
+ Assisting recovery of user data and DBMS data (e.g., transaction log); and
+ Tracking operations that users perform.
 Most commercial DBMS server applications also provide the following functions:
- A data model with which the DBMS data structures and organization can be
-conceptualized (e.g., hierarchical, object-oriented, relational data models) and
-DBMS objects defined.
- High-level language(s) or interfaces that allow authorized users to define
-database constructs; access and modify user or DBMS data; present user or
-DBMS data; and perform operations on those data.
+ A data model with which the DBMS data structures and organization can be conceptualized
+(e.g., hierarchical, object-oriented, relational data models) and DBMS objects defined.
+ High-level language(s) or interfaces that allow authorized users to define database
constructs;
+access and modify user or DBMS data; present user or DBMS data; and perform operations
on
+those data.
 A DBMS supports two user types:
-1. Users who interact with the DBMS to observe and/or modify data objects for
-which they have authorization to access; and
-2. The authorized administrators who implement and manage the various
-information-related policies of an organization (e.g., access, integrity,
-consistency, availability) for the databases that they install, configure, manage,
-and/or own.
+ Users who interact with the DBMS to observe and/or modify data objects for which they
have
+authorization to access; and
+ The authorized administrators who implement and manage the various information-related
+policies of an organization (e.g., access, integrity, consistency, availability) for the
databases that
+they install, configure, manage, and/or own.
 A DBMS stores and controls access to two types of data:
-1. The first type is the user data that the DBMS maintains and protects. User
-data may consist of the following:
-a) The user data stored in or as database objects;
-b) The definitions of user databases and database objects, commonly
-known as DBMS metadata; and
-c) The user-developed queries, functions, or procedures that the DBMS
-maintains for users.
-2. The second type is the DBMS data (e.g., configuration parameters, user
-security attributes, transaction log, audit instructions, and records) that the
-DBMS maintains and may use to operate the DBMS.
-DBMS specifications identify the detailed requirements for the DBMS server
-functions given in the above list.
-2.3.2 Security Functionality Provided by the TOE
+ The first type is the user data that the DBMS maintains and protects. User data may
```

```
consist of
+the following:
+ The user data stored in or as database objects;
+ The definitions of user databases and database objects, commonly known as DBMS
+metadata; and
+ The user-developed queries, functions, or procedures that the DBMS maintains for users.
+ The second type is the DBMS data (e.g., configuration parameters, user security
attributes,
+transaction log, audit instructions, and records) that the DBMS maintains and may use to
+operate the DBMS.
+DBMS specifications identify the detailed requirements for the DBMS server functions
given in the
+above list.
+1.3.2. Security Functionality Provided by the TOE
 A DBMS evaluated against this PP will provide the following security services.
 Security services that must be provided by the TOE:
- Discretionary Access Control (DAC) limits access to objects based on the
-identity of the subjects or groups to which the subjects and objects belong,
-and which allows authorized users to specify how the objects that they control
-are protected.
- Audit Capture for creation of information on all auditable events.
- Authorized administration role to allow authorized administrators to configure
-the policies for discretionary access control, identification and authentication,
-and auditing. The TOE must enforce the authorized administration role.
- Limitation of the number of concurrent sessions and restrictions on
-establishing sessions.
-Application Note 1: Some administrative tasks may be delegated to specific users (which
-by that delegation become administrators although they can only
-perform some limited administrative actions). Ensuring that those
-users cannot extend the administrative rights assigned to them is a
-security functionality the TOE has to provide.
-2.3.3 TOE definition
-The TOE consists of at least one instance of the security functions of the DBMS
-server application with its associated guidance documentation and the interfaces to
-the external Information Technology (IT) entities with which the DBMS interacts.
-This cPP does not dictate a specific architecture. The ST writer will need to identify
-and describe the TOE architecture to be evaluated. Architectures are described in
-section 1.4.2.
-The external IT entities, with which the DBMS may interact, may include the
+ Discretionary Access Control (DAC) limits access to objects based on the identity of
the subjects
+or groups to which the subjects and objects belong, and which allows authorized users to
+specify how the objects that they control are protected.
+ Audit Capture for creation of information on all auditable events.
+ Authorized administration role to allow authorized administrators to configure the
policies for
+discretionary access control, identification and authentication, and auditing. The TOE
must
```

```
+enforce the authorized administration role.
+ Limitation of the number of concurrent sessions and restrictions on establishing
sessions.
+Some administrative tasks may be delegated to specific users (which by that delegation
become
+administrators although they can only perform some limited administrative actions).
Ensuring that
+those users cannot extend the administrative rights assigned to them is a security
functionality the
+TOE has to provide.
+1.3.3. TOE definition
+The TOE consists of at least one instance of the security functions of the DBMS server
application
+with its associated guidance documentation and the interfaces to the external
Information
+Technology (IT) entities with which the DBMS interacts.
+This cPP does not dictate a specific architecture. The ST writer will need to identify
and describe the
+TOE architecture to be evaluated. Architectures are described in section 1.4.2.
+The external IT entities, with which the DBMS may interact, may include the following:
+ Client applications that allow users to interface with the DBMS server.
+ The host operating system (host OS) on which the TOE has been installed.
+ The networking, printing, data-storage, and other devices and services with which the
host OS
+may interact on behalf of the DBMS or the DBMS user; and the other IT products such as
+application servers, web servers, authentication servers, directory services, and
transaction
+processors with which the DBMS may interact to perform a DBMS function or a security
+function.
+The TOE Security Function (TSF) is limited to the elements required to exercise the
evaluated
+security functionality.
+The DBMS must specify the host OS on which it must reside to provide the desired degree
of
+security feature integration as well as the configuration of those OS(es) required to
support the
+DBMS functions. In all cases, the TOE must be installed and administered in accordance
with the
+TOE installation and administration instructions.
+1.3.4. Limitations of Security Claims
+Conformance with this cPP will not guarantee the following:
+ Physical protection mechanisms and the administrative procedures for using them are in
place.
+ Mechanisms to ensure the complete availability of the data residing on the DBMS are in
place.
+The DBMS can provide simultaneous access to data to make the data available to more than
one
+person at a given time, and it can enforce DBMS resource allocation limits to prevent
```

```
users from
+monopolizing a DBMS service/resource. However, it cannot detect or prevent the
unavailability
+that may occur because of a physical or environmental disaster, a storage device
failure, or
+external threats on the underlying operating system. For such threats to availability,
the
+environment must provide the required countermeasures.
+ Mechanisms to ensure that users properly secure the data that they retrieve from the
DBMS are
+in place. The security procedures of the organization(s) that use and manage the DBMS
must
+define users' data retrieval, storage, export, and disposition responsibilities.
+ Mechanisms to ensure that authorized administrators wisely use DAC. Although the DBMS
can
+support an access control policy by which users and optionally users in defined groups,
are
+granted access only to the data that they need to perform their jobs, it cannot
completely ensure
+that authorized administrators who are able to set access controls will do so prudently.
+1.4. TOE Operational Environment
+1.4.1. DBMS Architecture and Environmental Components
+This cPP does not dictate a specific architecture. A TOE compliant with this cPP may be
evaluated
+and may operate in several architectures, including, but not limited to, one or more of
the
 following:
- Client applications that allow users to interface with the DBMS server.
- The host operating system (host OS) on which the TOE has been installed;
- The networking, printing, data-storage, and other devices and services with
-which the host OS may interact on behalf of the DBMS or the DBMS user;
-and the other IT products such as application servers, web servers,
-authentication servers, directory services, and transaction processors with
-which the DBMS may interact to perform a DBMS function or a security
-function.
-The TOE Security Function (TSF) is limited to the elements required to exercise the
-evaluated security functionality.
-The DBMS must specify the host OS on which it must reside to provide the desired
-degree of security feature integration as well as the configuration of those OS(es)
-required to support the DBMS functions. In all cases, the TOE must be installed and
-administered in accordance with the TOE installation and administration instructions.
-2.3.4 Limitations of Security Claims
-Conformance with this cPP will not guarantee the following:
- Physical protection mechanisms and the administrative procedures for using
-them are in place.
- Mechanisms to ensure the complete availability of the data residing on the
-DBMS are in place. The DBMS can provide simultaneous access to data to
-make the data available to more than one person at a given time, and it can
```

```
-enforce DBMS resource allocation limits to prevent users from monopolizing a
-DBMS service/resource. However, it cannot detect or prevent the
-unavailability that may occur because of a physical or environmental disaster,
-a storage device failure, or external threats on the underlying operating
-system. For such threats to availability, the environment must provide the
-required countermeasures.
-• Mechanisms to ensure that users properly secure the data that they retrieve
-from the DBMS are in place. The security procedures of the organization(s)
-that use and manage the DBMS must define users' data retrieval, storage,
-export, and disposition responsibilities.
-• Mechanisms to ensure that authorized administrators wisely use DAC.
-Although the DBMS can support an access control policy by which users and
-optionally users in defined groups, are granted access only to the data that
-they need to perform their jobs, it cannot completely ensure that authorized
-administrators who are able to set access controls will do so prudently.
-2.4 TOE Operational Environment
-2.4.1 DBMS Architecture and Environmental Components
-This cPP does not dictate a specific architecture. A TOE compliant with this cPP may
-be evaluated and may operate in several architectures, including, but not limited to,
-one or more of the following:
-• A stand-alone system running the DBMS server application; a stand-alone
-system running the DBMS server and DBMS client(s) and serving one, or
-more than one, online user at a given time;
-• A network of systems communicating with several distributed DBMS servers
-simultaneously;
-• A network of workstations or terminals running DBMS clients and
-communicating with a DBMS server simultaneously; these devices may be
-hardwired to the host computer or be connected to it by means of local or
-wide-area networks; and
-• A network of workstations communicating with one or more application
-servers, which in turn interact with the DBMS on behalf of the workstation
-users or other subjects (e.g., a DBMS server interacting with a transaction
-processor that manages user requests).
-2.4.2 TOE Administration
-This cPP defines one necessary administrator role (authorized administrator) which
-is established by the developer of the DBMS. This cPP allows the DBMS developer
-or security target writer to define more user or administrator roles.
-If the security target allows it, the administrators of the system may assign privileges
-to users. When the DBMS is established, the ability to assign privileges and their
-associated responsibilities must also exist.
-Authorized administrators of the TOE will have capabilities that are commensurate
-with their assigned administrative privileges. The very ability to establish and assign
-privileges will itself be a privileged function.
-3. Conformance Claims
-3.1 Conformance with CC
-This cPP conforms to the requirements of Common Criteria v3.1, Revision 5 as
-defined by the references [CC1], [CC2] and [CC3]. The methodology applied for the
-PP evaluation is defined in [CEM].
```

```
-This cPP also applies the CC and CEM Addenda, Exact Conformance, Selection-
-Based SFRs, Optional SFRs: V2.0 dated 2021-Sep-30, Final.
-This cPP satisfies the following Assurance Families: APE_CCL.1, APE_ECD.1,
-APE_INT.1, APE_OBJ.2, APE_REQ.2 and APE_SPD.1.
-3.2 Conformance with CC parts 2 and 3
-DBMS cPP is CC version 3.1 revision 5 Part 2 extended and Part 3 conformant.
-3.3 Conformance with Packages
+ A stand-alone system running the DBMS server application; a stand-alone system running
the
+DBMS server and DBMS client(s) and serving one, or more than one, online user at a given
time;
+ A network of systems communicating with several distributed DBMS servers
simultaneously;
+ A network of workstations or terminals running DBMS clients and communicating with a
DBMS
+server simultaneously; these devices may be hardwired to the host computer or be
connected to
+it by means of local or wide-area networks; and
+ A network of workstations communicating with one or more application servers, which in
turn
+interact with the DBMS on behalf of the workstation users or other subjects (e.g., a
DBMS server
+interacting with a transaction processor that manages user requests).
+1.4.2. TOE Administration
+This cPP defines one necessary administrator role (authorized administrator) which is
established
+by the developer of the DBMS. This cPP allows the DBMS developer or security target
writer to
+define more user or administrator roles.
+If the security target allows it, the administrators of the system may assign privileges
to users.
+When the DBMS is established, the ability to assign privileges and their associated
responsibilities
+must also exist.
+Authorized administrators of the TOE will have capabilities that are commensurate with
their
+assigned administrative privileges. The very ability to establish and assign privileges
will itself be a
+privileged function.
+Chapter 2. Conformance Claims
+2.1. Conformance with CC
+This cPP conforms to the requirements of Common Criteria:2022 as defined by the
references [CC1],
+[CC2] and [CC3]. The framework for the specification of evaluation activities is defined
in [CC4], the
+assurance package is defined in [CC5], and the methodology applied for the PP evaluation
is defined
+in [CEM]. This cPP also accounts for errata and interpretations for CC:2022 and CEM:2022
```

```
[CCE].
+This cPP applies exact conformance, selection-based SFRs, and optional SFRs as defined
for CC:2022.
+This cPP satisfies the following Assurance Families: APE_CCL.1, APE_ECD.1, APE_INT.1,
APE_OBJ.2,
+APE_REQ.2 and APE_SPD.1.
+2.2. Conformance with CC parts 2 and 3
+DBMS cPP is CC:2022 Part 2 extended and Part 3 conformant.
+2.3. Conformance with Packages
 The DBMS cPP does not claim conformance to any functional packages.
-The DBMS cPP claims conformance to the EAL2 assurance package augmented by
+The DBMS cPP claims conformance to the EAL2 assurance package defined in [CC5],
augmented by
 ALC_FLR.3 Systematic flaw remediation.
-3.4 Conformance with other Protection Profiles
+2.4. Conformance with other Protection Profiles
 The DBMS cPP does not claim conformance to any other Protection Profile.
-3.5 Conformance Statement
+2.5. Conformance Statement
 DBMS cPP requires exact conformance by an ST.
-Exact Conformance is a subset of Strict Conformance as defined by [CC1]. Exact
-Conformance is defined as the ST containing all of the SFRs in section 6 (these are
-mandatory SFRs) of this cPP, and potentially SFRs from Appendix A (these are
-optional SFRs). While iteration is allowed, no additional requirements from [CC2],
-[CC3], or definitions of extended components not already included in this cPP) are
-allowed to be included in the ST. Further, no SFRs in section 6 of this cPP are
-allowed to be omitted.
-3.6 PP-Configuration
-The collaborative Protection Profile for Database Management Systems (DBMS cPP)
-is structured as a base Protection Profile, able to accommodate a set of (optional)
-PP-Modules.
-4. Security Problem Definition
-In this section, the security problem definition (SPD) for a DBMS is described. First,
-the informal discussion of the SPD is presented followed by a more formal
-description in terms of the identified threats, policies, and assumptions that will be
-used to identify the specific security requirements addressed by this cPP.
-4.1 Informal Discussion
-Given their common usage as repositories of high value data, attackers routinely
-target DBMS installations for compromise. Vulnerabilities that attackers may take
-advantage of are:
-• Design flaws and programming bugs in the DBMS and the associated
-programs and systems, creating various security vulnerabilities (e.g. weak or
-ineffective access controls) which can lead to data loss/corruption,
-performance degradation etc;
-• Unauthorized or unintended activity or misuse by authorized database users,
-or network/systems managers, or by unauthorized users or hackers (e.g.
-inappropriate access to sensitive data, metadata or functions within
-databases, or inappropriate changes to the database programs, structures or
```

```
-security configurations);
-  Malware infections causing incidents such as unauthorized access, leakage
-or disclosure of personal or proprietary data, deletion of or damage to the data
-or programs, interruption or denial of authorized access to the database,
-attacks on other systems and the unanticipated failure of database services;
-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.
-4.2 Assets and Threat Agents
-The threats given in section 4.3 refer to various threat agents and assets. The term
-"threat agent" is defined in CC Part 1.
-The assets, mentioned in Table 1 below, are either defined in CC Part 1, or in the
-glossary which will be provided in the Appendix of the cPP document.
-The terms "TSF data", "TSF" and "user data", are defined in CC Part 1. The terms
-"public objects" and "TOE resources" are given in the glossary which will be provided
-in the Appendix of the cPP document.
-4.3 Threats
-The following threats are identified and addressed by the TOE and should be read in
-conjunction with the threat rationale.
-Compliant TOEs will provide security functionality that addresses threats to the TOE
-and implements policies that are imposed by the organization, law or regulation.
-Table 1: Threats Applicable to the TOE
+Exact Conformance is a subset of Strict Conformance as defined by [CC1]. Exact
Conformance is
+defined as the ST containing all of the SFRs in section 6 (these are mandatory SFRs) of
this cPP,
+potentially SFRs from Appendix A (these are optional SFRs), and all applicable SFRs from
Appendix
+D that are required by selections made in the mandatory SFRs. While iteration is
allowed, no
+additional requirements from [CC2], [CC3], or definitions of extended components not
already
+included in this cPP) are allowed to be included in the ST. Further, no SFRs in section
6 of this cPP
+are allowed to be omitted.
+2.6. PP-Configuration
+The collaborative Protection Profile for Database Management Systems (DBMS cPP) is
structured as
+a base Protection Profile, able to accommodate a set of (optional) PP-Modules.
+Chapter 3. Security Problem Definition
+In this section, the security problem definition (SPD) for a DBMS is described. First,
the informal
+discussion of the SPD is presented followed by a more formal description in terms of the
identified
+threats, policies, and assumptions that will be used to identify the specific security
requirements
+addressed by this cPP.
```

```
+3.1. Informal Discussion
+Given their common usage as repositories of high value data, attackers routinely target
DBMS
+installations for compromise. Vulnerabilities that attackers may take advantage of are:
+ Design flaws and programming bugs in the DBMS and the associated programs and systems,
+creating various security vulnerabilities (e.g. weak or ineffective access controls)
which can lead
+to data loss/corruption, performance degradation etc;
+ Unauthorized or unintended activity or misuse by authorized database users, or
+network/systems managers, or by unauthorized users or hackers (e.g. inappropriate access
to
+sensitive data, metadata or functions within databases, or inappropriate changes to the
+database programs, structures or security configurations);
+ Malware infections causing incidents such as unauthorized access, leakage or disclosure
of
+personal or proprietary data, deletion of or damage to the data or programs,
interruption or
+denial of authorized access to the database, attacks on other systems and the
unanticipated
+failure of database services; and
+ Data corruption and/or loss caused by the entry of invalid data or commands, mistakes
in
+database or system administration processes, sabotage/criminal damage etc.
+3.2. Assets and Threat Agents
+The threats given in section 4.3 refer to various threat agents and assets. The term
"threat agent" is
+defined in CC Part 1.
+The assets, mentioned in Table 1 below, are either defined in CC Part 1, or in the
glossary which will
+be provided in the Appendix of the cPP document.
+The terms "TSF data", "TSF" and "user data", are defined in CC Part 1. The terms "public
objects" and
+"TOE resources" are given in the glossary which will be provided in the Appendix of the
cPP
+document.
+3.3. Threats
+The following threats are identified and addressed by the TOE and should be read in
conjunction
+with the threat rationale.
+Compliant TOEs will provide security functionality that addresses threats to the TOE and
+implements policies that are imposed by the organization, law or regulation.
+Table 1. Table 1: Threats Applicable to the TOE
 Threat Definition
-A user or a process may read or modify TSF data using
-T.ACCESS_TSFDATA functions of the TOE without being identified, authenticated
-and authorized.
-A user or a process may use, manage or modify the TSF,
-T.ACCESS_TSFFUNC
```

```
-bypassing the protection mechanisms of the TSF.
-A user who has not successfully completed identification
-T.IA_USER and authentication may gain unauthorized access to user
-data or TOE resources beyond public objects.
-A user or a process acting on behalf of a user may gain
-unauthorized access to user or TSF data through
-T.RESIDUAL_DATA
-reallocation of TOE resources from one user or process to
-another.
-An authenticated user or a process, in conflict with the
-T.UNAUTHORIZED_ACCESS TOE security policy, may gain unauthorized access to user
+T.ACCESS_TSFDATA A user or a process may read or modify TSF data
+using functions of the TOE without being
+identified, authenticated and authorized.
+T.ACCESS_TSFFUNC A user or a process may use, manage or modify
+the TSF, bypassing the protection mechanisms of
+the TSF.
+T.IA_USER A user who has not successfully completed
+identification and authentication may gain
+unauthorized access to user data or TOE
+resources beyond public objects.
+T.RESIDUAL_DATA A user or a process acting on behalf of a user
+may gain unauthorized access to user or TSF
+data through reallocation of TOE resources from
+one user or process to another.
+T.UNAUTHORIZED_ACCESS An authenticated user or a process, in conflict
+with the TOE security policy, may gain
+unauthorized access to user data.
+3.4. Organizational Security Policies
+The following organizational security policies are addressed by cPP-conformant TOEs:
+Table 2. Table 2: Policies Applicable to the TOE
+Policy Definition
+P.ACCOUNTABILITY The authorized users of the TOE shall be held
+accountable for their actions within the TOE.
+P.ROLES Administrative authority to TSF functionality
+shall be given to trusted personnel and be as
+restricted as possible while supporting only the
+administrative duties the person has. This role
+shall be separate and distinct from other
+authorized users.
+P.USER Authority shall only be given to users who are
+trusted to perform the actions correctly and are
+permitted by the organization to access user
 data.
-4.4 Organizational Security Policies
-The following organizational security policies are addressed by cPP-conformant
-TOEs:
-Table 2: Policies Applicable to the TOE
```

```
-Policy Definition
-The authorized users of the TOE shall be held accountable for
-P.ACCOUNTABILITY
-their actions within the TOE.
-Administrative authority to TSF functionality shall be given to
-trusted personnel and be as restricted as possible while
-P.ROLES
-supporting only the administrative duties the person has. This
-role shall be separate and distinct from other authorized users.
-Authority shall only be given to users who are trusted to
-P.USER perform the actions correctly and are permitted by the
-organization to access user data.
-4.5 Assumptions
-This section contains assumptions regarding the IT environment in which the TOE
-will reside.
-Table 3: Assumptions Applicable to the TOE Environment
+3.5. Assumptions
+This section contains assumptions regarding the IT environment in which the TOE will
reside.
+Table 3. Table 3: Assumptions Applicable to the TOE Environment
 Assumption Definition
 Physical aspects
-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
-A.PHYSICAL
-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.
+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
-Authorized users possess the necessary authorization to access the
-A.AUTHUSER information managed by the TOE in accordance with organization
-information access policies.
-The TOE security functionality is managed by one or more competent,
-authorized administrators. The system administrative personnel are not
-A.MANAGE
-careless, willfully negligent, or hostile, and will follow and abide by the
-instructions provided by the guidance documentation.
-Authorized users are sufficiently trained to accomplish a task or a group of
```

```
-A.TRAINEDUSER tasks within a secure IT environment by exercising control over their user
-data.
+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
-There are no general-purpose computing capabilities (e.g., compilers or
-A.NO_GENERAL_
-user applications) available on DBMS servers, other than those services
-PURPOSE
-necessary for the operation, administration, and support of the DBMS.
-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
-A.PEER_FUNC_& decisions are assumed to correctly implement the functionality used by
-_MGT the TSF consistent with the assumptions defined for this functionality and
-to be properly managed and operate under security policy constraints
+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.
-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
-A.SUPPORT
-capture, user authentication, and authorization that is used by the TOE is
-correct and up to date.
+Assumption Definition
```

```
+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
-All connections to and from remote trusted IT systems and between
-separate parts of the TSF are physically and/or logically protected within
-A.CONNECT the TOE environment to ensure the integrity and confidentiality of the data
-transmitted and to ensure the authenticity of the communication end
-points.
-5. Security Objectives
-This section identifies the security objectives of the TOE and its supporting
-environment.
-These security objectives identify the responsibilities of the TOE and its environment
-in meeting the security problem definition (SPD).
-5.1 TOE security objectives
-5.1.1 O.ADMIN_ROLE
-The TOE shall provide roles that allow only authorized users to have access to
-administrative privileges that are specific to the role.
-5.1.2 O.AUDIT_GENERATION
-The TOE shall provide the capability to detect and create/generate records of
-security relevant events associated with users.
-5.1.3 O.DISCRETIONARY_ACCESS
-The TSF shall control access of subjects and/or users to named resources based on
-identity of the object, subject, or user. The TSF shall allow authorized users to
-specify for each access mode which users/subjects are allowed to access a specific
-named object in that access mode.
-5.1.4 O.I&A
-The TOE shall ensure that users are authenticated before the TOE processes any
-actions that require authentication.
-5.1.5 O.MANAGE
-The TSF shall provide all the functions and facilities necessary to manage TOE
-security mechanisms, and shall restrict such management actions to authorized
-users.
-5.1.6 O.RESIDUAL_INFORMATION
-The TOE shall ensure that any information contained in a protected resource within
-its control is not inappropriately disclosed when the resource is reallocated.
-5.1.7 O.TOE_ACCESS
-The TOE shall provide functionality that controls a user's logical access to user data
-and to the TSF.
-5.2 Security Objectives for the Operational Environment
-5.2.1 OE.ADMIN
-Those responsible for the TOE are competent and trustworthy individuals, capable of
-managing the TOE and the security of the information it contains.
-5.2.2 OE.INFO_PROTECT
-Those responsible for the TOE shall establish and implement procedures to ensure
```

```
-that information is protected in an appropriate manner. In particular:
-  All network and peripheral cabling shall be approved for the transmittal of the
-most sensitive data transmitted over the link. Such physical links are assumed
-to be adequately protected against threats to the confidentiality and integrity
-of the data transmitted using appropriate physical and logical protection
-techniques.
-  DAC protections on security-relevant files (such as audit trails and
-authorization databases) shall always be set up correctly.
-  Users are authorized to access parts of the data managed by the TOE and
-are trained to exercise control over their own data.
-5.2.3 OE.NO_GENERAL_ PURPOSE
-There shall be no general-purpose computing capabilities (e.g., compilers or user
-applications) available on DBMS servers, other than those services necessary for
-the operation, administration, and support of the DBMS.
-5.2.4 OE.PHYSICAL
-Those responsible for the TOE shall ensure that those parts of the TOE critical to
-enforcement of the security policy are protected from physical attack that might
-compromise IT security objectives. The protection shall be commensurate with the
-value of the IT assets protected by the TOE.
-5.3 Security Objectives for the Operational IT Environment
-5.3.1 OE.IT_I&A
-Any information provided by a trusted entity in the environment and used to support
-user authentication and authorization used by the TOE is correct and up to date.
-5.3.2 OE.IT_TRUSTED_SYSTEM
-External IT systems may be required by the TOE for the enforcement of the security
-policy. These external trusted IT systems shall be managed according to known,
-accepted, and trusted policies based on the same rules and policies applicable to the
-TOE, and are physically and shall be sufficiently protected from any attack that may
-cause those functions to provide false results.
-6. Security Functional Requirements
+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.
+Chapter 4. Security Objectives
+This section identifies the security objectives of the TOE and its supporting
environment.
+These security objectives identify the responsibilities of the TOE and its environment
in meeting the
+security problem definition (SPD).
+4.1. TOE security objectives
+4.1.1. O.ADMIN_ROLE
+The TOE shall provide roles that allow only authorized users to have access to
administrative
+privileges that are specific to the role.
```

```
+4.1.2. O.AUDIT_GENERATION
+The TOE shall provide the capability to detect and create/generate records of security
relevant
+events associated with users.
+4.1.3. O.DISCRETIONARY_ACCESS
+The TSF shall control access of subjects and/or users to named resources based on
identity of the
+object, subject, or user. The TSF shall allow authorized users to specify for each
access mode which
+users/subjects are allowed to access a specific named object in that access mode.
+4.1.4. O.I&A
+The TOE shall ensure that users are authenticated before the TOE processes any actions
that
+require authentication.
+4.1.5. O.MANAGE
+The TSF shall provide all the functions and facilities necessary to manage TOE security
+mechanisms, and shall restrict such management actions to authorized users.
+4.1.6. O.RESIDUAL_INFORMATION
+The TOE shall ensure that any information contained in a protected resource within its
control is
+not inappropriately disclosed when the resource is reallocated.
+4.1.7. O.TOE_ACCESS
+The TOE shall provide functionality that controls a user's logical access to user data
and to the TSF.
+4.2. Security Objectives for the Operational
+Environment
+4.2.1. OE.ADMIN
+Those responsible for the TOE are competent and trustworthy individuals, capable of
managing the
+TOE and the security of the information it contains.
+4.2.2. OE.INFO_PROTECT
+Those responsible for the TOE shall establish and implement procedures to ensure that
information
+is protected in an appropriate manner. In particular:
+ All network and peripheral cabling shall be approved for the transmittal of the most
sensitive
+data transmitted over the link. Such physical links are assumed to be adequately
protected
+against threats to the confidentiality and integrity of the data transmitted using
appropriate
+physical and logical protection techniques.
+ DAC protections on security-relevant files (such as audit trails and authorization
databases)
+shall always be set up correctly.
+ Users are authorized to access parts of the data managed by the TOE and are trained to
exercise
+control over their own data.
+4.2.3. OE.NO_GENERAL_ PURPOSE
```

```
+There shall be no general-purpose computing capabilities (e.g., compilers or user
applications)
+available on DBMS servers, other than those services necessary for the operation,
administration,
+and support of the DBMS.
+4.2.4. OE.PHYSICAL
+Those responsible for the TOE shall ensure that those parts of the TOE critical to
enforcement of the
+security policy are protected from physical attack that might compromise IT security
objectives.
+The protection shall be commensurate with the value of the IT assets protected by the
TOE.
+4.3. Security Objectives for the Operational IT
+Environment
+4.3.1. OE.IT_I&A
+Any information provided by a trusted entity in the environment and used to support user
+authentication and authorization used by the TOE is correct and up to date.
+4.3.2. OE.IT_TRUSTED_SYSTEM
+External IT systems may be required by the TOE for the enforcement of the security
policy. These
+external trusted IT systems shall be managed according to known, accepted, and trusted
policies
+based on the same rules and policies applicable to the TOE, and are physically and shall
be
+sufficiently protected from any attack that may cause those functions to provide false
results.
+Chapter 5. Security Functional
+Requirements
 The individual security functional requirements are specified in the sections below.
-6.1 Class: Security Audit (FAU)
-6.1.1 Audit Data Generation (FAU_GEN)
+5.1. Class: Security Audit (FAU)
+5.1.1. Audit Data Generation (FAU_GEN)
 FAU_GEN.1 Audit data generation
 FAU_GEN.1.1
-The TSF shall be able to generate an audit record of the following auditable events:
-a) Start-up and shutdown of the audit functions;
-b) All auditable events for the minimum level of audit listed in Table 4:
-Auditable Events; and
-c) [Start-up and shutdown of the DBMS; and
-d) Use of special permissions (e.g., those often used by authorized
-administrators to circumvent access control policies).]
+The TSF shall be able to generate audit data of the following auditable events:
+ Start-up and shutdown of the audit functions;
+ All auditable events for the [selection: minimum] level of audit listed in Table 4:
Auditable
+Events; and
+ [assignment: Start-up and shutdown of the DBMS; and use of special permissions (e.g.,
```

```
those
+often used by authorized administrators to circumvent access control policies).]
 FAU_GEN.1.2
-The TSF shall record within each audit record at least the following information:
-a) Date and time of the event, type of event, subject identity (if applicable), and
-the outcome (success or failure) of the event; and
-b) For each audit event type, based on the auditable event definitions of the
-functional components included in the cPP/ST, [information specified in
-column three of Table 4: Auditable Events].
-Application Note 2: In column 3 of the table below, "Additional Audit Record Contents"
is
-used to designate data that should be included in the audit record if it
-"makes sense" in the context of the event which generates the record.
-If no other information is required (other than that listed in item a)
-above) for a particular auditable event type, then an assignment of
-"none" is acceptable.
-Table 4: Auditable Events
-Column 1: Column 2: Column 3:
-Security Functional Auditable Event(s) Additional Audit Record
-Requirement Contents
+The TSF shall record within the audit data at least the following information:
+ Date and time of the auditable event, type of event, subject identity (if applicable),
and the
+outcome (success or failure) of the event; and
+ For each auditable event type, based on the auditable event definitions of the
functional
+components included in the PP, PP-Module, functional package or ST, [assignment:
information
+specified in column three of Table 4: Auditable Events].
+Application Note 1: In column 3 of the table below, "Additional Audit Data Contents" is
used to
+designate data that should be included in the audit data if it "makes sense" in the
context of the event
+which generates the data. If no other information is required (other than that listed in
item a) above)
+for a particular auditable event type, then an assignment of "none" is acceptable.
+Table 4. Table 4: Auditable Events
+Column 1: Security Functional Column 2: Auditable Event(s) Column 3: Additional Audit
+Requirement Data Contents
 FAU_GEN.1 None None
 FAU_GEN.2 None None
-FAU_SEL.1 All modifications to the audit The identity of the
-configuration that occur authorized administrator
-Column 1: Column 2: Column 3:
-Security Functional Auditable Event(s) Additional Audit Record
-Requirement Contents
-while the audit collection that made the change to the
-functions are operating audit configuration
```

```
+Column 1: Security Functional Column 2: Auditable Event(s) Column 3: Additional Audit
+Requirement Data Contents
+FAU_SEL.1 All modifications to the audit The identity of the authorized
+configuration that occur while administrator that made the
+the audit collection functions change to the audit
+are operating configuration
 FDP_ACC.1 None None
-FDP_ACF.1 Successful requests to None
-perform an operation on an
-object covered by the SFP
+FDP_ACF.1 Successful requests to perform None
+an operation on an object
+covered by the SFP
 FDP_RIP.1 None None
 FIA_ATD.1 None None
-FIA_UAU.2 Access denied by None
-authentication mechanism
-FIA_UID.2 Access denied by The user identity provided
-authentication mechanism
-FMT_MSA.1 None None
+FIA_UAU.2 Access denied by authentication None
+mechanism
+FIA_UID.2 Access denied by authentication The user identity provided
+mechanism
+FMT_MSA.1(1) None None
+FMT_MSA.1(2) None None
 FMT_MSA.3 None None
 FMT_MTD.1 None None
 FMT_REV.1(1) Unsuccessful revocation of Identity of individual
-security attributes attempting to revoke
-security attributes
+security attributes attempting to revoke security
+attributes
 FMT_REV.1(2) Unsuccessful revocation of Identity of individual
-security attributes attempting to revoke
-security attributes
+security attributes attempting to revoke security
+attributes
 FMT_SMF.1 Use of the management Identity of the administrator
 functions performing these functions
 FMT_SMR.1 Modifications to the group of Identity of authorized
 users that are part of a role administrator modifying the
 role definition
 FPT_TRC.1 Restoring consistency None
-FTA_MCS.1 Rejection of a new session None
+FTA_MCS_EXT.1 Rejection of a new session None
 based on the limitation of
 multiple concurrent sessions
```

```
 FTA_TSE.1 Denial of a session Identity of the individual
@@ -697,1340 +580,1240 @@
 mechanism
 FAU_GEN.2 User identity association
 FAU_GEN.2.1
-For audit events resulting from actions of identified users and any identified groups,
-the TSF shall be able to associate each auditable event with the identity of the
-[selection: "user", "user and group"] that caused the event.
-6.1.2 Security audit event selection (FAU_SEL)
+For audit events resulting from actions of identified users and any identified groups, the TSF shall
+be able to associate each auditable event with the identity of the [selection: user, user and group]
+that caused the event.
+5.1.2. Security audit event selection (FAU_SEL)
 FAU_SEL.1 Selective audit
 FAU_SEL.1.1
-The TSF shall be able to select the set of events to be audited from the set of all
-auditable events based on the following attributes:
-a) user identity;
-b) [selection: object identity, user identity, subject identity, host identity, group
-identity, event type, success of auditable security events, failure of
-auditable security events];
-c) [assignment: list of additional attributes that audit selectivity is based upon].
-Application Note 3: "event type" is to be defined by the ST author; the intent is to be able
-to include or exclude classes of audit events.
-Application Note 4: The intent of this requirement is to capture sufficient audit data to
-allow the administrators to perform their tasks; additional audit data
-may be captured.
-6.2 Class: User Data Protection (FDP)
-6.2.1 Access control policy (FDP_ACC)
+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:
+ user identity;
+ [selection: object identity, user identity, subject identity, host identity, group identity, event
+type, success of auditable security events, failure of auditable security events];
+ [assignment: list of additional attributes that audit selectivity is based upon].
+Application Note 2: "event type" is to be defined by the ST author; the intent is to be able to include or
+exclude classes of audit events.
+Application Note 3: The intent of this requirement is to capture sufficient audit data to allow the
+administrators to perform their tasks; additional audit data may be captured.
+5.2. Class: User Data Protection (FDP)
```

```
+5.2.1. Access control policy (FDP_ACC)
 FDP_ACC.1 Subset access control
 FDP_ACC.1.1
-The TSF shall enforce the [Discretionary Access Control policy] to objects on [all
+The TSF shall enforce the [assignment: Discretionary Access Control policy] on
[assignment: all
 subjects, all DBMS-controlled objects, and all operations among them].
+5.2.2. Access control functions (FDP_ACF)
 FDP_ACF.1 Security attribute based access control
 FDP_ACF.1.1
-The TSF shall enforce the [Discretionary Access Control policy] to objects based on
-the following: [assignment: list of subjects and objects controlled under the indicated
-SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-
-relevant security attributes].
-Application Note 5: DBMS-controlled objects may be implementation-specific objects that
-are presented to authorized users at the user interface to the DBMS.
-They may include, but are not limited to tables, records, files, indexes,
-views, constraints, stored queries, and metadata. Data structures that
-are not presented to authorized users at the DBMS user interface, but
-are used internally, are internal TSF data structures. Internal TSF data
-structures are not controlled according to the rules specified in
+The TSF shall enforce the [assignment: Discretionary Access Control policy] to objects
based on the
+following: [assignment: list of subjects and objects controlled under the indicated SFP,
and for each,
+the SFP-relevant security attributes, or named groups of SFP-relevant security
attributes].
+Application Note 4: DBMS-controlled objects may be implementation-specific objects that
are
+presented to authorized users at the user interface to the DBMS. They may include, but
are not limited
+to tables, records, files, indexes, views, constraints, stored queries, and metadata.
Data structures that
+are not presented to authorized users at the DBMS user interface, but are used
internally, are internal
+TSF data structures. Internal TSF data structures are not controlled according to the
rules specified in
 FDP_ACF.1.
-Application Note 6: Named groups of security attributes can be specified to provide a
-convenient means to refer to multiple security attributes. In this PP,
-'Named group of SFP-relevant security attributes' refers to a group of
-attributes that can be associated with an object or a subject. For
+Application Note 5: Named groups of security attributes can be specified to provide a
convenient
+means to refer to multiple security attributes. In this PP, 'Named group of SFP-relevant
security
+attributes' refers to a group of attributes that can be associated with an object or a
subject. For
```

```
 example, this could be a named Access Control List (ACL).
 FDP_ACF.1.2
-The TSF shall enforce the following rules to determine if an operation among
-controlled subjects and controlled objects is allowed: [assignment: rules governing
-access among controlled subjects and controlled objects using controlled operations
-on controlled objects].
+The TSF shall enforce the following rules to determine if an operation among controlled
subjects
+and controlled objects is allowed: [assignment: rules governing access among controlled
subjects
+and controlled objects using controlled operations on controlled objects].
 FDP_ACF.1.3
-The TSF shall explicitly authorize access of subjects to objects based on the
-following additional rules: [assignment: rules, based on security attributes, that
-explicitly authorize access of subjects to objects].
+The TSF shall explicitly authorize access of subjects to objects based on the following
additional
+rules: [assignment: rules, based on security attributes, that explicitly authorize
access of subjects to
+objects].
 FDP_ACF.1.4
-The TSF shall explicitly deny access of subjects to objects based on the following
-additional rules: [assignment: rules, based on security attributes, that explicitly deny
-access of subjects to objects].
-6.2.2 Residual information protection (FDP_RIP)
+The TSF shall explicitly deny access of subjects to objects based on the following
additional rules:
+[assignment: rules, based on security attributes, that explicitly deny access of
subjects to objects].
+5.2.3. Residual information protection (FDP_RIP)
 FDP_RIP.1 Subset residual information protection
 FDP_RIP.1.1
-The TSF shall ensure that any previous information content of a resource is made
-unavailable upon the allocation of the resource to the following objects: [assignment:
-list of objects].
-6.3 Class: Identification and authentication (FIA)
-Application Note 7: It is drawn to the attention of the ST writer that the
identification and
-authentication family was written in such a way that the SFRs might
-be used in either the case that Identification and Authentication (I&A)
-services are performed by the TOE itself or that they are performed
-within the TOE environment.
-6.3.1 User authentication (FIA_UAU)
+The TSF shall ensure that any previous information content of a resource is made
unavailable upon
+the [selection: allocation of the resource to] the following objects: [assignment: list
of objects].
+5.3. Class: Identification and authentication (FIA)
```

```
+Application Note 6: It is drawn to the attention of the ST writer that the
identification and
+authentication family was written in such a way that the SFRs might be used in either
the case that
+Identification and Authentication (I&A) services are performed by the TOE itself or that
they are
+performed within the TOE environment.
+5.3.1. User authentication (FIA_UAU)
 FIA_UAU.2 User authentication before any action
 FIA_UAU.2.1
-The TSF shall require each user to be successfully authenticated before allowing
-any other TSF-mediated actions on behalf of that user.
-6.3.2 User attribute definition (FIA_ATD)
+The TSF shall require each user to be successfully authenticated before allowing any
other TSF-
+mediated actions on behalf of that user.
+5.3.2. User attribute definition (FIA_ATD)
 FIA_ATD.1 User attribute definition
 FIA_ATD.1.1
-The TSF shall maintain the following list of security attributes belonging to individual
-users:
-a) Database user identifier and any associated group memberships;
-b) Security-relevant database roles; and
-c) [assignment: list of security attributes].
-Application Note 8: The intent of this requirement is to specify the TOE security
attributes
-that the TOE utilizes to determine access. These attributes may be
-controlled by the environment or by the TOE itself.
-6.3.3 User identification (FIA_UID)
+The TSF shall maintain the following list of security attributes belonging to individual
users:
+ Database user identifier and any associated group memberships;
+ Security-relevant database roles; and
+ [assignment: list of security attributes].
+Application Note 7: The intent of this requirement is to specify the TOE security
attributes that the
+TOE utilizes to determine access. These attributes may be controlled by the environment
or by the TOE
+itself.
+5.3.3. User identification (FIA_UID)
 FIA_UID.2 User identification before any action
 FIA_UID.2.1
-The TSF shall require each user to be successfully identified before allowing any
-other TSF-mediated actions on behalf of that user.
-6.4 Class: Security management (FMT)
-6.4.1 Management of security attributes (FMT_MSA)
-FMT_MSA.1 Management of security attributes
-FMT_MSA.1.1
```

```
-The TSF shall enforce the [Discretionary Access Control policy] to restrict the ability
-to [manage] all the security attributes [assignment: list of security attributes] to
-[authorized administrators].
+The TSF shall require each user to be successfully identified before allowing any other
TSF-
+mediated actions on behalf of that user.
+5.4. Class: Security management (FMT)
+5.4.1. Management of security attributes (FMT_MSA)
+FMT_MSA.1(1) Management of security attributes (Users)
+FMT_MSA.1.1(1)
+The TSF shall enforce the [assignment: Discretionary Access Control policy] to restrict
the ability to
+[selection: [assignment: manage]] the security attributes [assignment: associated with
users] to
+[assignment: authorized administrators].
+FMT_MSA.1(2) Management of security attributes (Objects)
+FMT_MSA.1.1(2)
+The TSF shall enforce the [assignment: Discretionary Access Control policy] to restrict
the ability to
+[selection: [assignment: manage]] the security attributes [assignment: associated with
objects] to
+[assignment: authorized administrators, authorized users].
 FMT_MSA.3 Static attribute initialization
 FMT_MSA.3.1
-The TSF shall enforce the [Discretionary Access Control policy] to provide restrictive
-default values for security attributes that are used to enforce the SFP.
-Application Note 9: This requirement applies to new objects at the top-level (e.g.,
tables).
-When lower-level objects are created (e.g., rows, cells), these may
-inherit the permissions of the top-level objects by default. In other
-words, the permissions of the 'child' objects can take the permissions
-of the 'parent' objects by default.
+The TSF shall enforce the [assignment: Discretionary Access Control policy] to provide
[selection:
+restrictive] default values for security attributes that are used to enforce the SFP.
+Application Note 8: This requirement applies to new objects at the top-level (e.g.,
tables). When lower-
+level objects are created (e.g., rows, cells), these may inherit the permissions of the
top-level objects by
+default. In other words, the permissions of the 'child' objects can take the permissions
of the 'parent'
+objects by default.
 FMT_MSA.3.2
-The TSF shall allow the [no user] to specify alternative initial values to override the
+The TSF shall allow the [assignment: 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)
```

```
+5.4.2. Management of TSF data (FMT_MTD)
 FMT_MTD.1 Management of TSF data
 FMT_MTD.1.1
-The TSF shall restrict the ability to [include or exclude] the [auditable events] to
-[authorized administrators].
-6.4.3 Revocation (FMT_REV)
-FMT_REV.1(1) Revocation
+The TSF shall restrict the ability to [selection: [assignment: include or exclude]] the
[assignment:
+auditable events] to [assignment: authorized administrators].
+5.4.3. Revocation (FMT_REV)
+FMT_REV.1(1) Revocation (Users)
 FMT_REV.1.1(1)
-The TSF shall restrict the ability to revoke [assignment: list of security attributes]
-associated with the users under the control of the TSF to [the authorized
-administrator].
+The TSF shall restrict the ability to revoke [assignment: list of security attributes]
associated with
+the [selection: users] under the control of the TSF to [assignment: authorized
administrator].
 FMT_REV.1.2(1)
 The TSF shall enforce the rules [assignment: specification of revocation rules].
-FMT_REV.1(2) Revocation (DAC)
+FMT_REV.1(2) Revocation (Objects)
 FMT_REV.1.1(2)
-The TSF shall restrict the ability to revoke [assignment: list of security attributes]
-associated with the objects under the control of the TSF to [the authorized
-administrator] and database users with sufficient privileges as allowed by the
-Discretionary Access Control policy.
+The TSF shall restrict the ability to revoke [assignment: list of security attributes]
associated with
+the [selection: objects] under the control of the TSF to [assignment: authorized
administrator,
+authorized users].
 FMT_REV.1.2(2)
 The TSF shall enforce the rules [assignment: specification of revocation rules].
-6.4.4 Specification of management functions (FMT_SMF)
+5.4.4. Specification of management functions (FMT_SMF)
 FMT_SMF.1 Specification of Management Functions
 FMT_SMF.1.1
-The TSF shall be capable of performing the following security management
-functions:
-[
-• Database configuration
-• User and role management
-[selection:
-• Management of groups
-• Adding or removing a database
```

```
-  Revocation of security attributes
-  Configuration of the maximum number of concurrent sessions
-  Configuration of session establishment rules
-  Configuration of TSF replication and consistency
-  Configuration of TOE access information rules
-  No other security management functions]
-[assignment: any additional security management functions required to
-configure the claimed security]
-].
-Application Note 10: The ST author should ensure that all security attributes identified
in
-FIA_ATD.1 are adequately managed and protected.
-6.4.5 Security management roles (FMT_SMR)
+The TSF shall be capable of performing the following security management functions:
[assignment:
+Database configuration; User and role management; Configure the session limiting
mechanism;
+[selection: Management of groups, Adding or removing a database, Revocation of security
+attributes, Configuration of session establishment rules, Configuration of TSF
replication and
+consistency, Configuration of TOE access information rules, No other security management
+functions]; [assignment: any additional security management functions required to
configure the
+claimed security]].
+Application Note 9: The ST author should ensure that all security attributes identified
in FIA_ATD.1
+are adequately managed and protected.
+5.4.5. Security management roles (FMT_SMR)
 FMT_SMR.1 Security roles
 FMT_SMR.1.1
-The TSF shall maintain the roles [authorized administrator and [assignment:
-additional authorized identified roles]].
+The TSF shall maintain the roles [assignment: authorized administrator, authorized
users, and
+[assignment: additional authorized identified roles]].
 FMT_SMR.1.2
 The TSF shall be able to associate users with roles.
-Application Note 11: This requirement identifies a minimum set of management roles. An
-ST may describe, or an operational environment may contain a finer-
-grain decomposition of roles that correspond to the roles identified
-here (e.g., database non-administrative user or database operator).
-The ST author may change the names of the roles identified above
-but the "new" roles must still perform the functions that the security
-management requirements in this cPP have defined. It is not
-necessary to list roles that are not exercised in the evaluated
-configuration.
-6.5 Class: TOE access (FTA)
-6.5.1 Limitation on multiple concurrent sessions (FTA_MCS)
```

```
-FTA_MCS.1 Basic limitation on multiple concurrent sessions
-FTA_MCS.1.1
-The TSF shall restrict the maximum number of concurrent sessions that belong to
-the same user.
-FTA_MCS.1.2
-The TSF shall enforce, by default, a limit of [assignment: default number] sessions
-per user.
-Application Note 12: The ST author is reminded that the CC part 2, [CC2] para 473 allows
-that the default number may be defined as a management function in
-FMT.
-6.5.2 TOE session establishment (FTA_TSE)
+Application Note 10: The authorized users role defined in FMT_SMR.1.1 is referenced in
+FMT_REV.1.1(2) and FMT_MSA.1.1(2) for objects.
+Application Note 11: This requirement identifies a minimum set of management roles. An
ST may
+describe, or an operational environment may contain a finer-grain decomposition of roles
that
+correspond to the roles identified here (e.g., database non-administrative user or
database operator).
+The ST author may change the names of the roles identified above but the "new" roles
must still
+perform the functions that the security management requirements in this cPP have
defined. It is not
+necessary to list roles that are not exercised in the evaluated configuration.
+5.5. Class: TOE access (FTA)
+5.5.1. Configurable Session Limiting Mechanisms (FTA_MCS_EXT)
+FTA_MCS_EXT.1 Configurable Session Limiting Mechanisms
+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 mechanism(s).
+Application Note 12: If "User session locking as defined by FTA_MCS.1" is selected in
+FTA_MCS_EXT.1.1, then FTA_MCS.1 must also be included from Appendix D.
+5.5.2. TOE session establishment (FTA_TSE)
 FTA_TSE.1 TOE session establishment
 FTA_TSE.1.1
-The TSF shall be able to deny session establishment based on [assignment:
-attributes that can be set explicitly by authorized administrator(s), including
-user identity, and [selection: group identity, time of day, day of the week,
-[assignment: list of additional attributes]]].
-7. Security Assurance Requirements
-The Security Objectives for the TOE in section 5 were constructed to address threats
```

```
-identified in section 4. The Security Functional Requirements (SFRs) in section 6 are
-a formal instantiation of the Security Objectives. This cPP identifies the Security
-Assurance Requirements (SARs) to frame the extent to which the evaluator
-assesses the documentation applicable for the evaluation and performs independent
-testing.
-This section lists the set of SARs from CC part 3 [CC3] that are required in
-evaluations against this cPP. Individual Evaluation Activities to be performed are
-specified in [SD].
-The general model for evaluation of TOEs against STs written to conform to this cPP
-is as follows:
-After the ST has been approved for evaluation, the IT Security Evaluation Facility
-(ITSEF) will obtain the TOE, supporting environmental IT (if required), and the
-administrative/user guides for the TOE. The ITSEF is expected to perform actions
-mandated by the Common Evaluation Methodology [CEM] for the ASE and ALC
-SARs. The ITSEF also performs the Evaluation Activities contained within the [SD],
-which are derived from the [CEM] assurance requirements as they apply to the
-specific technology instantiated in the TOE. The Evaluation Activities that are
-captured in the [SD] also provide clarification as to what the developer needs to
-provide to demonstrate the TOE is compliant with the cPP.
+The TSF shall be able to deny session establishment based on [assignment: attributes
that can be set
+explicitly by authorized administrator(s), including user identity, and [selection:
group identity,
+time of day, day of the week, [assignment: list of additional attributes]]].
+Chapter 6. Security Assurance Requirements
+The Security Objectives for the TOE in section 5 were constructed to address threats
identified in
+section 4. The Security Functional Requirements (SFRs) in section 6 are a formal
instantiation of the
+Security Objectives. This cPP identifies the Security Assurance Requirements (SARs) to
frame the
+extent to which the evaluator assesses the documentation applicable for the evaluation
and
+performs independent testing.
+This section lists the set of SARs from CC part 3 [CC3] that are required in evaluations
against this
+cPP. Individual Evaluation Activities to be performed are specified in [SD].
+The general model for evaluation of TOEs against STs written to conform to this cPP is
as follows:
+After the ST has been approved for evaluation, the IT Security Evaluation Facility
(ITSEF) will
+obtain the TOE, supporting environmental IT (if required), and the administrative/user
guides for
+the TOE. The ITSEF is expected to perform actions mandated by the Common Evaluation
+Methodology [CEM] for the ASE and ALC SARs. The ITSEF also performs the Evaluation
Activities
+contained within the [SD], which are derived from the [CEM] assurance requirements as
they apply
```

```
+to the specific technology instantiated in the TOE. The Evaluation Activities that are
captured in the
+[SD] also provide clarification as to what the developer needs to provide to demonstrate
the TOE is
+compliant with the cPP.
 The TOE security assurance requirements are identified in Table 5.
-Table 5: Security Assurance Requirements
+Table 5. Table 5: Security Assurance Requirements
 Assurance Class Assurance Components
 Security Target (ASE) Conformance claims (ASE_CCL.1)
 Extended components definition (ASE_ECD.1)
 ST introduction (ASE_INT.1)
-Security objectives for the operational environment (ASE_OBJ.2)
+Security objectives for the operational
+environment (ASE_OBJ.2)
 Stated security requirements (ASE_REQ.2)
 Security Problem Definition (ASE_SPD.1)
 TOE summary specification (ASE_TSS.1)
 Development (ADV) Security architecture description (ADV_ARC.1)
 Basic functional specification (ADV_FSP.2)
 Basic design (ADV_TDS.1)
-Guidance documents Operational user guidance (AGD_OPE.1)
-(AGD)
+Guidance documents (AGD) Operational user guidance (AGD_OPE.1)
 Preparative procedures (AGD_PRE.1)
 Life cycle support (ALC) Labeling of the TOE (ALC_CMC.2)
 TOE CM coverage (ALC_CMS.2)
 Delivery procedures (ALC_DEL.1)
+Assurance Class Assurance Components
 Flaw reporting procedures (ALC_FLR.3)
 Tests (ATE) Evidence of coverage (ATE_COV.1)
 Functional testing (ATE_FUN.1)
 Independent testing - sample (ATE_IND.2)
-Vulnerability assessment Vulnerability survey (AVA_VAN.2)
-(AVA)
-7.1 Class ASE: Security Target
-NOTE: The Supporting Document [SD] contains evaluation activities that refine the
-evaluation activities given in [CEM].
-7.2 Class ADV: Development
-NOTE: The Supporting Document [SD] contains evaluation activities that refine the
-evaluation activities given in [CEM].
-7.3 Class AGD: Guidance Documentation
-NOTE: The Supporting Document [SD] contains evaluation activities that refine the
-evaluation activities given in [CEM].
-7.4 Class ALC: Life-cycle Support
-NOTE: The Supporting Document [SD] contains evaluation activities that refine the
-evaluation activities given in [CEM].
-7.5 Class ATE: Tests
```

```
-NOTE: The Supporting Document [SD] contains evaluation activities that refine the
-evaluation activities given in [CEM].
-7.6 Class AVA: Vulnerability Assessment
-NOTE: The Supporting Document [SD] contains evaluation activities that refine the
-evaluation activities given in [CEM].
-A.Optional Requirements
-As indicated in the introduction to this cPP, the baseline requirements (those that
-must be performed by the TOE) are contained in the body of this cPP. Additionally,
-there is another type of requirements specified in Appendix A
-These requirements can be included in the ST, but do not have to be in order for a
-TOE to claim conformance to this cPP.
-ST authors are free to choose none, some or all SFRs defined in this chapter. It is
-not a requirement to add the SFRs defined in this chapter, even if the functionality is
-supported by the product.
-A.1 Class: Identification and authentication (FIA)
-A.1.1 Enhanced user-subject binding (FIA_USB_EXT)
+Vulnerability assessment (AVA) Vulnerability survey (AVA_VAN.2)
+6.1. Class ASE: Security Target
+6.2. Class ADV: Development
+6.3. Class AGD: Guidance Documentation
+6.4. Class ALC: Life-cycle Support
+6.5. Class ATE: Tests
+6.6. Class AVA: Vulnerability Assessment
+Appendix A: Optional Requirements
+As indicated in the introduction to this cPP, the baseline requirements (those that must
be
+performed by the TOE) are contained in the body of this cPP. Additionally, there is
another type of
+requirements specified in Appendix A
+These requirements can be included in the ST, but do not have to be in order for a TOE
to claim
+conformance to this cPP.
+ST authors are free to choose none, some or all SFRs defined in this chapter. It is not
a requirement
+to add the SFRs defined in this chapter, even if the functionality is supported by the
product.
+A.1. Class: Identification and authentication (FIA)
+A.1.1. Enhanced user-subject binding (FIA_USB_EXT)
 FIA_USB_EXT.2 Enhanced user-subject binding
-FIA_USB_EXT.2 .1
-The TSF shall associate the following user security attributes with subjects acting on
-the behalf of that user: [assignment: list of user security attributes].
-FIA_USB_EXT.2 .2
-The TSF shall enforce the following rules on the initial association of user security
-attributes with subjects acting on the behalf of users: [assignment: rules for the
initial
-association of attributes].
-FIA_USB_EXT.2 .3
```

```
-The TSF shall enforce the following rules governing changes to the user security
-attributes associated with subjects acting on the behalf of users: [assignment: rules
-for the changing of attributes].
-FIA_USB_EXT.2 .4
-The TSF shall enforce the following rules for the assignment of subject security
-attributes not derived from user security attributes when a subject is created:
-[assignment: rules for the initial association of the subject security attributes not
-derived from user security attributes].
-Application Note 13: Some administrative tasks may be delegated to specific users (which
-by that delegation become administrators although they can only
-perform some limited administrative actions). Ensuring that those
-users cannot extend the administrative rights assigned to them is a
+FIA_USB_EXT.2.1
+The TSF shall associate the following user security attributes with subjects acting on
the behalf of
+that user: [assignment: list of user security attributes].
+FIA_USB_EXT.2.2
+The TSF shall enforce the following rules on the initial association of user security
attributes with
+subjects acting on the behalf of users: [assignment: rules for the initial association
of attributes].
+FIA_USB_EXT.2.3
+The TSF shall enforce the following rules governing changes to the user security
attributes
+associated with subjects acting on the behalf of users: [assignment: rules for the
changing of
+attributes].
+FIA_USB_EXT.2.4
+The TSF shall enforce the following rules for the assignment of subject security
attributes not
+derived from user security attributes when a subject is created: [assignment: rules for
the
+initial association of the subject security attributes not derived from user security
+attributes].
+Application Note 13: Some administrative tasks may be delegated to specific users (which
by that
+delegation become administrators although they can only perform some limited
administrative
+actions). Ensuring that those users cannot extend the administrative rights assigned to
them is a
 security functionality the TOE has to provide.
-Application Note 14: If FIA_USB_EXT.2 is included in an ST then Table 4: Auditable
Events
-is refined to add the following entry:
-Column 1: Column 2: Column 3:
-Security Functional Auditable Event(s) Additional Audit Record
-Requirement Contents
+Application Note 14: If FIA_USB_EXT.2 is included in an ST then Table 4: Auditable
```

```
Events is refined to
+add the following entry:
+Column 1: Security Functional Column 2: Auditable Event(s) Column 3: Additional Audit
+Requirement Data Contents
 FIA_USB_EXT.2 Unsuccessful binding of user None
-security attributes to a
-subject (e.g. creation of a
-subject)
-A.2 Class: Protection of the TSF (FPT)
-A.2.1 Internal TOE TSF data replication consistency (FPT_TRC)
+security attributes to a subject
+(e.g. creation of a subject)
+A.2. Class: Protection of the TSF (FPT)
+A.2.1. Internal TOE TSF data replication consistency (FPT_TRC)
 FPT_TRC.1 Internal TSF consistency
 FPT_TRC.1.1
-The TSF shall ensure that TSF data is consistent when replicated between parts of
-the TOE.
+The TSF shall ensure that TSF data is consistent when replicated between parts of the
TOE.
 FPT_TRC.1.2
-When parts of the TOE containing replicated TSF data are disconnected, the TSF
-shall ensure the consistency of the replicated TSF data upon reconnection before
-processing any requests for [assignment: list of functions dependent on TSF data
-replication consistency].
-Application Note 15: In general, it is impossible to achieve complete, constant
consistency of
-TSF data that is distributed to remote portions of a TOE because
-distributed portions of the TSF may be active at different times or
-disconnected from one another. This requirement attempts to address this
-situation in a practical manner by acknowledging that there will be TSF
-data inconsistencies but that they will be corrected without undue delay.
-For example, a TSF could provide timely consistency through periodic
-broadcast of TSF data to all TSF nodes maintaining replicated TSF data.
-Another example approach is for the TSF to provide a mechanism to
-explicitly probe remote TSF nodes for inconsistencies and respond with
-action to correct the identified inconsistencies.
-A.3 Class: TOE access (FTA)
-A.3.1 TOE access information (FTA_TAH_EXT)
+When parts of the TOE containing replicated TSF data are disconnected, the TSF shall
ensure the
+consistency of the replicated TSF data upon reconnection before processing any requests
for
+[assignment: list of functions dependent on TSF data replication consistency].
+Application Note 15: In general, it is impossible to achieve complete, constant
consistency of TSF data
+that is distributed to remote portions of a TOE because distributed portions of the TSF
may be active
```

```
+at different times or disconnected from one another. This requirement attempts to
address this
+situation in a practical manner by acknowledging that there will be TSF data
inconsistencies but that
+they will be corrected without undue delay. For example, a TSF could provide timely
consistency
+through periodic broadcast of TSF data to all TSF nodes maintaining replicated TSF data.
Another
+example approach is for the TSF to provide a mechanism to explicitly probe remote TSF
nodes for
+inconsistencies and respond with action to correct the identified inconsistencies.
+A.3. Class: TOE access (FTA)
+A.3.1. TOE access information (FTA_TAH_EXT)
 FTA_TAH_EXT.1 TOE access information
 FTA_TAH_EXT.1.1
 Upon a session establishment attempt, the TSF shall store
-a) the date and time of the session establishment attempt of the user.
-b) the incremental count of successive unsuccessful session establishment
+ the date and time of the session establishment attempt of the user.
+ the incremental count of successive unsuccessful session establishment
 attempt(s).
 FTA_TAH_EXT.1.2
 Upon successful session establishment, the TSF shall allow the date and time of
-a) the previous last successful session establishment, and
-b) the last unsuccessful attempt to session establishment and the number of
-unsuccessful attempts since the previous last successful session
-establishment to be retrieved by the user.
-Application Note 16: If FTA_TAH_EXT.1 is included in an ST then Table 4: Auditable
-Events is refined to add the following entry:
-Column 1: Column 2: Column 3:
-Security Functional Auditable Event(s) Additional Audit Record
-Requirement Contents
+ the previous last successful session establishment, and
+ the last unsuccessful attempt to session establishment and the number of unsuccessful
attempts
+since the previous last successful session establishment to be retrieved by the user.
+Application Note 16: If FTA_TAH_EXT.1 is included in an ST then Table 4: Auditable
Events is refined to
+add the following entry:
+Column 1: Security Functional Column 2: Auditable Event(s) Column 3: Additional Audit
+Requirement Data Contents
 FTA_TAH_EXT.1 None None
-B.Extended Component Definitions
-This appendix contains the definitions for the extended requirements that are used in
-the cPP, including those used in Appendix A.
-B.1 Class: User Identification and Authentication (FIA)
-B.1.1 Enhanced user-subject binding (FIA_USB_EXT)
-Family Behaviour
```

```
-FIA_USB_EXT.2 is analogous to FIA_USB.1 except that it adds the possibility to
-specify rules whereby subject security attributes are also derived from TSF data
-other than user security attributes.
-Component levelling
+Chapter 7. Extended Component Definitions
+This appendix contains the definitions for the extended requirements that are used in
the cPP,
+including those used in Appendix A.
+7.1. Class: User Identification and Authentication (FIA)
+7.1.1. Enhanced user-subject binding (FIA_USB_EXT)
+7.1.1.1. Family Behaviour
+FIA_USB_EXT.2 is analogous to FIA_USB.1 except that it adds the possibility to specify
rules whereby
+subject security attributes are also derived from TSF data other than user security
attributes.
+7.1.1.2. Component levelling
 FIA_USB_EXT.2 is hierarchical to FIA_USB.1.
-Management
+Figure 1. Component levelling
+7.1.1.3. Management
 See management description specified for FIA_USB.1 in [CC2].
-Audit
+7.1.1.4. Audit
 See audit requirement specified for FIA_USB.1 in [CC2].
 FIA_USB_EXT.2 Enhanced user-subject binding
 Hierarchical to: FIA_USB.1 User-subject binding
 Dependencies: FIA_ATD.1 User attribute definition
 FIA_USB_EXT.2.1
-The TSF shall associate the following user security attributes with subjects acting on
-the behalf of that user: [assignment: list of user security attributes].
+The TSF shall associate the following user security attributes with subjects acting on
the behalf of
+that user: [assignment: list of user security attributes].
 FIA_USB_EXT.2.2
-The TSF shall enforce the following rules on the initial association of user security
-attributes with subjects acting on the behalf of users: [assignment: rules for the
initial
-association of attributes].
+The TSF shall enforce the following rules on the initial association of user security
attributes with
+subjects acting on the behalf of users: [assignment: rules for the initial association
of attributes].
 FIA_USB_EXT.2.3
-The TSF shall enforce the following rules governing changes to the user security
-attributes associated with subjects acting on the behalf of users: [assignment: rules
-for the changing of attributes].
+The TSF shall enforce the following rules governing changes to the user security
attributes
```

```
+associated with subjects acting on the behalf of users: [assignment: rules for the
changing of
+attributes].
 FIA_USB_EXT.2.4
-The TSF shall enforce the following rules for the assignment of subject security
-attributes not derived from user security attributes when a subject is created:
-[assignment: rules for the initial association of the subject security attributes not
-derived from user security attributes].
-B.2 Class: TOE access (FTA)
-B.2.1 TOE access information (FTA_TAH_EXT)
-Family Behaviour
-FTA_TAH_EXT.1 TOE access information provides the requirement for a TOE to
-make available information related to attempts to establish a session.
-Component levelling
+The TSF shall enforce the following rules for the assignment of subject security
attributes not
+derived from user security attributes when a subject is created: [assignment: rules for
the
+initial association of the subject security attributes not derived from user security
+attributes].
+7.2. Class: TOE access (FTA)
+7.2.1. Limitation on multiple concurrent sessions (FTA_MCS_EXT)
+7.2.1.1. Family Behaviour
+This family defines requirements to place limits on the number of concurrent sessions.
+7.2.1.2. Component levelling
+FTA_MCS_EXT.1 is not hierarchical to any other components.
+Figure 2. Component levelling
+7.2.1.3. Management
+The following actions could be considered for the management functions in FMT:
+ management of the maximum allowed number of concurrent user sessions
+ management of the enforcement mechanism(s)
+7.2.1.4. Audit
+The following actions should be auditable if FAU_GEN Security audit data generation is
included in
+the PP/ST:
+ rejection of a new session based on the limitation of multiple concurrent sessions
+7.2.1.5. Dependencies
+FIA_UID.2 User identification before any action
+FTA_MCS_EXT.1 Configurable Session Limiting Mechanisms
+Hierarchical to: No other components.
+Dependencies: FIA_UID.2 User identification before any action
+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 mechanism(s).
+7.2.2. TOE access information (FTA_TAH_EXT)
+7.2.2.1. Family Behaviour
+FTA_TAH_EXT.1 TOE access information provides the requirement for a TOE to make
available
+information related to attempts to establish a session.
+7.2.2.2. Component levelling
 FTA_TAH_EXT.1 is not hierarchical to any other components.
-Management:
+Figure 3. Component levelling
+7.2.2.3. Management
 There are no management activities foreseen.
-Audit:
+7.2.2.4. Audit
 There are no auditable events foreseen.
 FTA_TAH_EXT.1 TOE access information
 Hierarchical to: No other components.
 Dependencies: No dependencies.
 FTA_TAH_EXT.1.1
 Upon a session establishment attempt, the TSF shall store
-a) the date and time of the session establishment attempt of the user.
-b) the incremental count of successive unsuccessful session establishment
-attempt(s).
+ the date and time of the session establishment attempt of the user.
+ the incremental count of successive unsuccessful session establishment attempt(s).
 FTA_TAH_EXT.1.2
 Upon successful session establishment, the TSF shall allow the date and time of
-a) the previous last successful session establishment, and
-b) the last unsuccessful attempt to session establishment and the number of
-unsuccessful attempts since the previous last successful session
-establishment
+ the previous last successful session establishment, and
+ the last unsuccessful attempt to session establishment and the number of unsuccessful
attempts
+since the previous last successful session establishment
 to be retrieved by the user.
-C. Rationales
-C.1 TOE Security Objectives Coverage
-The table below gives a summary of the policies, and threats relating to the TOE
-security objectives.
-Table 6: Coverage of Security Objectives for the TOE
+Chapter 8. Rationales
+8.1. TOE Security Objectives Coverage
+The table below gives a summary of the policies, and threats relating to the TOE
security objectives.
+Table 6. Table 6: Coverage of Security Objectives for the TOE
```

```
 Objective Name SPD coverage
-O.ADMIN_ROLE P.ACCOUNTABILITY
-P.ROLES
-T.ACCESS_TSFFUNC
+O.ADMIN_ROLE P.ACCOUNTABILITY P.ROLES T.ACCESS_TSFFUNC
 O.AUDIT_GENERATION P.ACCOUNTABILITY
-O.DISCRETIONARY_ACCESS T.IA_USER
-T.UNAUTHORIZED_ACCESS
-O.I&A P.ACCOUNTABILITY
-T.ACCESS_TSFFUNC
-T.ACCESS_TSFDATA
-T.IA_USER
-O.MANAGE P.USER
-T.ACCESS_TSFDATA
-T.ACCESS_TSFFUNC
+O.DISCRETIONARY_ACCESS T.IA_USER T.UNAUTHORIZED_ACCESS
+O.I&A P.ACCOUNTABILITY T.ACCESS_TSFFUNC
+T.ACCESS_TSFDATA T.IA_USER
+O.MANAGE P.USER T.ACCESS_TSFDATA T.ACCESS_TSFFUNC
 T.UNAUTHORIZED_ACCESS
 O.RESIDUAL_INFORMATION T.RESIDUAL_DATA
-O.TOE_ACCESS P.ACCOUNTABILITY
-P.ROLES
-P.USER
-T.ACCESS_TSFDATA
-T.ACCESS_TSFFUNC
-T.IA_USER
-T.UNAUTHORIZED_ACCESS
-C.2 Rationale for TOE Security Objectives
+O.TOE_ACCESS P.ACCOUNTABILITY P.ROLES P.USER
+T.ACCESS_TSFDATA T.ACCESS_TSFFUNC
+T.IA_USER T.UNAUTHORIZED_ACCESS
+8.2. Rationale for TOE Security Objectives
 The table below gives the rationale for the TOE security objectives.
-Table 7: Rationale for the TOE Security Objectives
+Table 7. Table 7: Rationale for the TOE Security Objectives
 Threat/Policy TOE Security Objectives Rationale
 Addressing the Threat/Policy
-P.ACCOUNTABILITY O.ADMIN_ROLE O.ADMIN_ROLE
-The authorized users The TOE shall provide roles that supports this policy by ensuring
that
-of the TOE shall be allow only authorized users to the TOE provides a means of
-held accountable for have access to administrative granting authorized administrators
-their actions within privileges that are specific to the the privileges needed for
secure
-the TOE. role. administration.
-O.AUDIT_GENERATION O.AUDIT_GENERATION
-The TOE shall provide the supports this policy by ensuring that
```

```
-capability to generate records of audit records are generated to
-security relevant events enable accountability.
-associated with users.
-O.I&A O.I&A
-The TOE shall ensure that users supports this policy by requiring that
-are authenticated before the TOE each entity interacting with the TOE
-processes any actions that require is properly identified and
-authentication. authenticated before allowing any
-action.
-O.TOE_ACCESS O.TOE_ACCESS
-The TOE shall provide supports this policy by providing a
-mechanisms that control a user's mechanism for controlling user
-logical access to user data and to access.
-the TSF.
+P.ACCOUNTABILITY The O.ADMIN_ROLE The TOE shall O.ADMIN_ROLE supports this
+authorized users of the TOE provide roles that allow only policy by ensuring that the
TOE
+shall be held accountable for authorized users to have access provides a means of
granting
+their actions within the TOE. to administrative privileges that authorized
administrators the
+are specific to the role. privileges needed for secure
+administration.
+O.AUDIT_GENERATION The TOE O.AUDIT_GENERATION
+shall provide the capability to supports this policy by ensuring
+generate records of security that audit data is generated to
+relevant events associated with enable accountability.
+users.
 Threat/Policy TOE Security Objectives Rationale
 Addressing the Threat/Policy
-P.USER O.MANAGE O.MANAGE
-Authority shall only be The TSF shall provide all the supports this policy by ensuring
-given to users who functions and facilities necessary to that the functions and
facilities
-are trusted to perform manage TOE security mechanisms, supporting secure management
-the actions correctly and shall restrict such management are in place.
-and are permitted by actions to authorized users.
-the organization to
-O.TOE_ACCESS O.TOE_ACCESS
-access user data.
-The TOE shall provide mechanisms supports this policy by providing a
-that control a user's logical access to mechanism for controlling user
+O.I&A The TOE shall ensure that O.I&A supports this policy by
+users are authenticated before requiring that each entity
+the TOE processes any actions interacting with the TOE is
+that require authentication. properly identified and
+authenticated before allowing
+any action.
```

```
+O.TOE_ACCESS The TOE shall O.TOE_ACCESS supports this
+provide mechanisms that policy by providing a
+control a user's logical access to mechanism for controlling user
 user data and to the TSF. access.
 Threat/Policy TOE Security Objectives Rationale
 Addressing the Threat/Policy
-OE.ADMIN OE.ADMIN
-Those responsible for the TOE are supports this policy by ensuring
-competent and trustworthy that only competent administrators
-individuals, capable of managing the are allowed to manage the TOE.
-TOE and ensuring the security of
+P.USER Authority shall only be O.MANAGE The TSF shall O.MANAGE supports this policy
+given to users who are trusted provide all the functions and by ensuring that the
functions
+to perform the actions correctly facilities necessary to manage and facilities
supporting secure
+and are permitted by the TOE security mechanisms, and management are in place.
+organization to access user shall restrict such management
+data. actions to authorized users.
+O.TOE_ACCESS The TOE shall O.TOE_ACCESS supports this
+provide mechanisms that policy by providing a
+control a user's logical access to mechanism for controlling user
+user data and to the TSF. access.
+OE.ADMIN Those responsible OE.ADMIN supports this policy
+for the TOE are competent and by ensuring that only
+trustworthy individuals, competent administrators are
+capable of managing the TOE allowed to manage the TOE.
+and ensuring the security of
 information it contains.
 Threat/Policy TOE Security Objectives Rationale
 Addressing the Threat/Policy
-P.ROLES O.ADMIN_ROLE O.ADMIN_ROLE
-Administrative The TOE shall provide roles that supports this objective by
-authority to TSF allow only authorized users to have providing roles that allow only
-functionality shall be access to administrative privileges authorized users access to
-given to trusted that are specific to the role. administrative privileges.
-personnel and be as
-restricted as
-possible while O.TOE_ACCESS O.TOE_ACCESS
-supporting only the The TOE shall provide mechanisms supports this policy by controlling
-administrative duties that control a user's logical access access to TSF functionality
based
-the person has. This to user data and to the TSF. on role.
-role shall be
-separate and distinct
-from other
-authorized users.
+P.ROLES Administrative O.ADMIN_ROLE The TOE shall O.ADMIN_ROLE supports this
```

```
+authority to TSF functionality provide roles that allow only objective by providing
roles
+shall be given to trusted authorized users to have access that allow only authorized
+personnel and be as restricted to administrative privileges that users access to
administrative
+as possible while supporting are specific to the role. privileges.
+only the administrative duties
+the person has. This role shall
+be separate and distinct from
+other authorized users.
 Threat/Policy TOE Security Objectives Rationale
 Addressing the Threat/Policy
-T.ACCESS O.I&A O.I&A
-_TSFDATA
-The TOE shall ensure that users are supports this policy by requiring
-A user or a process authenticated before the TOE that each entity interacting with the
-may read or modify processes any actions that require TOE is properly identified and
-TSF data using authentication. authenticated before allowing any
-functions of the action the TOE is defined to provide
-TOE without being to authenticated users only.
-identified,
-O.MANAGE O.MANAGE
-authenticated and
-authorized. The TSF shall provide all the diminishes this threat since it
-functions and facilities necessary to ensures that functions and facilities
-manage TOE security mechanisms, used to modify TSF data are not
-and shall restrict such management available to unauthorized users.
-actions to authorized users.
-O.TOE_ACCESS O.TOE_ACCESS
-The TOE shall provide mechanisms mitigates this threat by restricting
-that control a user's logical access to TOE access.
+O.TOE_ACCESS The TOE shall O.TOE_ACCESS supports this
+provide mechanisms that policy by controlling access to
+control a user's logical access to TSF functionality based on role.
 user data and to the TSF.
 Threat/Policy TOE Security Objectives Rationale
 Addressing the Threat/Policy
-T.ACCESS O.ADMIN_ROLE O.ADMIN_ROLE
-_TSFFUNC
-The TOE will provide roles that allow mitigates this threat by restricting
-A user or a process only authorized users to have access access to privileged actions.
-may use, manage or to administrative privileges that are
-modify the TSF, specific to the role.
-bypassing the
-O.I&A O.I&A
-protection
-mechanisms of the The TOE shall ensure that users are mitigates this threat since the
-TSF. authenticated before the TOE TOE requires successful
```

```
-processes any actions that require authentication to the TOE prior to
-authentication. gaining access to any controlled-
-access content.
-O.MANAGE O.MANAGE
-The TSF shall provide all the functions mitigates this threat by ensuring
-and facilities necessary to manage that management functions are
-TOE security mechanisms, and shall restricted to authorized users.
-restrict such management actions to
-authorized users.
-O.TOE_ACCESS O.TOE_ACCESS
-The TOE shall provide mechanisms mitigates this threat by restricting
-that control a user's logical access to TOE access.
+T.ACCESS + _TSFDATA A user or O.I&A The TOE shall ensure that O.I&A supports this policy
by
+a process may read or modify users are authenticated before requiring that each entity
+TSF data using functions of the the TOE processes any actions interacting with the TOE
is
+TOE without being identified, that require authentication. properly identified and
+authenticated and authorized. authenticated before allowing
+any action the TOE is defined to
+provide to authenticated users
+only.
+O.MANAGE The TSF shall O.MANAGE diminishes this
+provide all the functions and threat since it ensures that
+facilities necessary to manage functions and facilities used to
+TOE security mechanisms, and modify TSF data are not
+shall restrict such management available to unauthorized users.
+actions to authorized users.
+O.TOE_ACCESS The TOE shall O.TOE_ACCESS mitigates this
+provide mechanisms that threat by restricting TOE access.
+control a user's logical access to
 user data and to the TSF.
-Threat/Policy TOE Security Objectives Addressing Rationale
-the Threat/Policy
-T.IA_USER O.DISCRETIONARY_ACCESS O.DISCRETIONARY_ACCESS
-A user who has not The TSF shall control access of mitigates this threat by requiring
-successfully subjects and/or users to named that data, including user data
-completed resources based on identity of the stored with the TOE, is protected
-identification and object, subject, or user. The TSF shall by discretionary access
controls.
-authentication may allow authorized users to specify for
-gain unauthorized each access mode which
-access to user data users/subjects are allowed to access a
-or TOE resources specific named object in that access
-beyond public mode.
-objects.
-O.I&A O.I&A
-The TOE shall ensure that users are mitigates this threat by requiring
```

```
-authenticated before the TOE that each entity interacting with
-processes any actions that require the TOE is properly identified
-authentication. and authenticated before
-allowing access beyond public
-objects.
-O.TOE_ACCESS O.TOE_ACCESS
-The TOE shall provide mechanisms mitigates this threat by
-that control a user's logical access to controlling logical access to user
-Threat/Policy TOE Security Objectives Addressing Rationale
-the Threat/Policy
-user data and to the TSF. data and TSF data.
 Threat/Policy TOE Security Objectives Rationale
 Addressing the Threat/Policy
-T.RESIDUAL O.RESIDUAL_INFORMATION O.RESIDUAL_INFORMATION
-_DATA The TOE shall ensure that any mitigates this threat by ensuring
-A user or a process information contained in a protected that data is not improperly
-acting on behalf of a resource is not inappropriately disclosed.
-user may gain disclosed when the resource is
-unauthorized access reallocated.
-to user or TSF data
-through reallocation
-of TOE resources
-from one user or
+T.ACCESS + _TSFFUNC A user or O.ADMIN_ROLE The TOE will O.ADMIN_ROLE mitigates this
+a process may use, manage or provide roles that allow only threat by restricting access
to
+modify the TSF, bypassing the authorized users to have access privileged actions.
+protection mechanisms of the to administrative privileges that
+TSF. are specific to the role.
+O.I&A The TOE shall ensure that O.I&A mitigates this threat since
+users are authenticated before the TOE requires successful
+the TOE processes any actions authentication to the TOE prior
+that require authentication. to gaining access to any
+controlled-access content.
+Threat/Policy TOE Security Objectives Rationale
+Addressing the Threat/Policy
+O.MANAGE The TSF shall O.MANAGE mitigates this threat
+provide all the functions and by ensuring that management
+facilities necessary to manage functions are restricted to
+TOE security mechanisms, and authorized users.
+shall restrict such management
+actions to authorized users.
+O.TOE_ACCESS The TOE shall O.TOE_ACCESS mitigates this
+provide mechanisms that threat by restricting TOE access.
+control a user's logical access to
+user data and to the TSF.
+Threat/Policy TOE Security Objectives Rationale
+Addressing the Threat/Policy
```

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

```
-to manage TOE security authorized users.
-mechanisms, and shall restrict
-such management actions to
-authorized users.
-O.TOE_ACCESS O.TOE_ACCESS
-The TOE shall provide mitigates this threat by controlling
-mechanisms that control a user's logical access to user data and TSF
-logical access to user data and to data.
-the TSF.
-C.3 Rationale for the Environmental Security Objectives
-The table below gives a summary of the assumptions, policies, and threats relating
-to the environmental security objectives.
-Table 8: Coverage of SPF Items for the TOE Environment Security Objectives
+T.UNAUTHORIZED + _ACCESS O.DISCRETIONARY_ACCESS The O.DISCRETIONARY_ACCESS
+An authenticated user or a TSF shall control access of mitigates this threat by
+process, in conflict with the TOE subjects and/or users to named requiring that data,
including
+security policy, may gain resources based on identity of TSF data, is protected by
+unauthorized access to user the object, subject or user. The discretionary access
controls.
+data. 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.MANAGE The TSF shall O.MANAGE mitigates this threat
+provide all the functions and by ensuring that access to user
+facilities necessary to manage data is restricted to authorized
+TOE security mechanisms, and users.
+shall restrict such management
+actions to authorized users.
+O.TOE_ACCESS The TOE shall O.TOE_ACCESS mitigates this
+provide mechanisms that threat by controlling logical
+control a user's logical access to access to user data and TSF
+user data and to the TSF. data.
+8.3. Rationale for the Environmental Security
+Objectives
+The table below gives a summary of the assumptions, policies, and threats relating to
the
+environmental security objectives.
+Table 8. Table 8: Coverage of SPF Items for the TOE Environment Security Objectives
 Objective Name SPD coverage
-OE.ADMIN A.MANAGE
-P.USER
-OE.INFO_PROTECT A.AUTHUSER
-A.CONNECT
-A.MANAGE
```

```
-A.PHYSICAL
-A.TRAINEDUSER
-P.USER
+OE.ADMIN A.MANAGE + P.USER
+Objective Name SPD coverage
+OE.INFO_PROTECT A.AUTHUSER + A.CONNECT + A.MANAGE +
+A.PHYSICAL + A.TRAINEDUSER + P.USER +
 T.UNAUTHORIZED_ACCESS
 OE.IT_I&A A.SUPPORT
-OE.IT_TRUSTED_SYSTEM A.CONNECT
-A.PEER_FUNC_&_MGT
+OE.IT_TRUSTED_SYSTEM A.CONNECT + A.PEER_FUNC_&_MGT
 OE.NO_GENERAL_ PURPOSE A.NO_GENERAL_PURPOSE
-OE.PHYSICAL A.CONNECT
-A.PHYSICAL
+OE.PHYSICAL A.CONNECT + A.PHYSICAL
 The table below provides a rationale for the environmental security objectives.
-Table 9: Rationale for Environmental Security Objectives
-Assumption Environmental Objective Addressing Rationale for Specifying the
-the Assumption Environmental Security
+Table 9. Table 9: Rationale for Environmental Security Objectives
+Assumption Environmental Objective Rationale for Specifying the
+Addressing the Assumption Environmental Security
 Objective
-A.AUTHUSER OE.INFO_PROTECT OE.INFO_PROTECT
-Authorized users Those responsible for the TOE shall supports the assumption by
-possess the establish and implement procedures to ensuring that users are
-necessary ensure that information is protected in authorized to access data
-authorization to an appropriate manner. In particular: managed by the TOE.
-access the
-  All network and peripheral cabling
-information
-shall be approved for the transmittal
-managed by the
-of the most sensitive data
-TOE in
+A.AUTHUSER Authorized users OE.INFO_PROTECT Those OE.INFO_PROTECT supports the
+possess the necessary responsible for the TOE shall assumption by ensuring that
+authorization to access the establish and implement users are authorized to access
+information managed by the procedures to ensure that data managed by the TOE.
+TOE in accordance with information is protected in an
+organization information appropriate manner. In
+access policies. particular: All network and
+peripheral cabling shall be
+approved for the transmittal of
+the most sensitive data
 transmitted over the link. Such
-accordance with
```

```
-physical links are assumed to be
-organization
-adequately protected against threats
-information
-to the confidentiality and integrity of
-access policies.
-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
+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.
-Assumption Environmental Objective Addressing Rationale for Specifying the
-the Assumption Environmental Security
+Assumption Environmental Objective Rationale for Specifying the
+Addressing the Assumption Environmental Security
 Objective
-A.CONNECT OE.INFO_PROTECT OE.INFO_PROTECT
-All connections to Those responsible for the TOE shall supports the assumption by
-and from remote establish and implement procedures to requiring that all network and
-trusted IT ensure that information is protected in peripheral cabling must be
-systems and an appropriate manner. In particular: approved for the transmittal of the
-between separate most sensitive data transmitted
- All network and peripheral cabling
-parts of the TSF over the link. Such physical links
-shall be approved for the transmittal
-are physically are assumed to be adequately
-of the most sensitive data
-and/or logically protected against threats to the
```

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

```
-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
+OE.PHYSICAL Those responsible OE.PHYSICAL supports the
+for the TOE shall ensure that assumption by ensuring that
+those parts of the TOE critical to appropriate physical security is
+enforcement of the security provided within the domain.
+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.
+A.SUPPORT Any information OE.IT_I&A Any information OE.IT_I&A supports the
+provided by a trusted entity in provided by a trusted entity in assumption implicitly.
+the IT environment and used to the environment and used to
+support the provision of time support user authentication
+and date, information used in and authorization used by the
+audit capture, user TOE is correct and up to date.
+authentication, and
+authorization that is used by
+the TOE is correct and up to
 date.
-A.MANAGE OE.ADMIN OE.ADMIN
-The TOE security Those responsible for the TOE are supports the assumption by
-functionality is competent and trustworthy individuals, requiring that authorized
-managed by one capable of managing the TOE and the administrators are competent,
-or more security of information it contains. thereby ensuring that all the tasks
-competent, are performed correctly and
-authorized effectively.
-administrators.
-OE.INFO_PROTECT OE.INFO_PROTECT
-The system
-administrative Those responsible for the TOE shall supports the assumption by
-personnel are not establish and implement procedures to ensuring that users are
-careless, willfully ensure that information is protected in authorized to access the
-negligent, or an appropriate manner. In particular: appropriate data, and are trained
-hostile, and will  All network and peripheral cabling to exercise control.
-follow and abide shall be approved for the transmittal
```

```
-by the of the most sensitive data
-instructions transmitted over the link. Such
-provided by the physical links are assumed to be
-guidance adequately protected against threats
-documentation. to the confidentiality and integrity of
-the data transmitted using
-appropriate physical and logical
-protection techniques.
- DAC protections on security-relevant
-files (such as audit trails and
-authentication databases) shall
-always be set up correctly.
- Users are authorized to access parts
-of the data managed by the TOE
-and are trained to exercise control
+A.MANAGE The TOE security OE.ADMIN Those responsible OE.ADMIN supports the
+functionality is managed by one for the TOE are competent and assumption by requiring
that
+or more competent, authorized trustworthy individuals, authorized administrators are
+administrators. The system capable of managing the TOE competent, thereby ensuring
+administrative personnel are and the security of information that all the tasks are
performed
+not careless, willfully negligent, it contains. correctly and effectively.
+or hostile, and will follow and
+abide by the instructions
+provided by the guidance
+documentation.
+Assumption Environmental Objective Rationale for Specifying the
+Addressing the Assumption Environmental Security
+Objective
+OE.INFO_PROTECT Those OE.INFO_PROTECT supports the
+responsible for the TOE shall assumption by ensuring that
+establish and implement users are authorized to access
+procedures to ensure that the appropriate data, and are
+information is protected in an trained to exercise control.
+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.
-Assumption Environmental Objective Addressing Rationale for Specifying the
-the Assumption Environmental Security
+A.NO_GENERAL + _PURPOSE OE.NO_GENERAL_PURPOSE OE.NO_GENERAL_PURPOSE The
+There are no general-purpose There shall be no general- DBMS server must not include
+computing capabilities (e.g., purpose computing capabilities any general-purpose
computing
+compilers or user applications) (e.g., compilers or user capabilities. This will protect
+available on DBMS servers, applications) available on the TSF data from malicious
+other than those services DMBS servers, other than those processes.
+necessary for the operation, services necessary for the
+administration, and support of operation, administration, and
+the DBMS. support of the DBMS.
+Assumption Environmental Objective Rationale for Specifying the
+Addressing the Assumption Environmental Security
 Objective
-A.NO_GENERAL OE.NO_GENERAL_PURPOSE OE.NO_GENERAL_PURPOSE
-_PURPOSE There shall be no general-purpose The DBMS server must not
-There are no computing capabilities (e.g., compilers include any general-purpose
-general-purpose or user applications) available on DMBS computing capabilities. This
will
-computing servers, other than those services protect the TSF data from
-capabilities (e.g., necessary for the operation, malicious processes.
-compilers or user administration, and support of the
-applications) DBMS.
-available on
-DBMS servers,
-other than those
-services
-necessary for the
-operation,
-administration,
-and support of
-the DBMS.
-A.PEER_FUNC_ OE.IT_TRUSTED_SYSTEM OE.IT_TRUSTED_SYSTEM
-&_MGT External IT systems may be required by supports this assumption by
-All external the TOE for the enforcement of the ensuring that remote systems
-trusted IT security policy. These external trusted supporting the TOE are managed
-systems trusted IT systems shall be managed according in a manner consistent with the
-by the TSF to to known, accepted, and trusted policies security policies applicable to
the
```

```
-provide TSF data based on the same rules and policies TOE.
-or services to the applicable to the TOE, and shall be
-TOE, or to sufficiently protected from any attack
-support the TSF that may cause those functions to
-in the provide false results.
-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.
-Assumption Environmental Objective Addressing Rationale for Specifying the
-the Assumption Environmental Security
+A.PEER_FUNC_&_MGT All OE.IT_TRUSTED_SYSTEM OE.IT_TRUSTED_SYSTEM
+external trusted IT systems External IT systems may be supports this assumption by
+trusted by the TSF to provide required by the TOE for the ensuring that remote systems
+TSF data or services to the TOE, enforcement of the security supporting the TOE are
+or to support the TSF in the policy. These external trusted IT managed in a manner
+enforcement of security policy systems shall be managed consistent with the security
+decisions are assumed to according to known, accepted, policies applicable to the TOE.
+correctly implement the and trusted policies based on
+functionality used by the TSF the same rules and policies
+consistent with the assumptions applicable to the TOE, and shall
+defined for this functionality be sufficiently protected from
+and to be properly managed any attack that may cause those
+and operate under security functions to provide false
+policy constraints compatible results.
+with those of the TOE.
+A.PHYSICAL The operational OE.PHYSICAL Those responsible OE.PHYSICAL supports this
+environment is assumed to for the TOE shall ensure that assumption by ensuring that
+provide the TOE with those parts of the TOE critical to the parts of the TOE critical to
+appropriate physical protection enforcement of the security the enforcement of the
security
+such that the TOE is not subject policy are protected from policy are protected from
+to physical attack that may physical attack that might physical attack.
```

```
+compromise the security and/or compromise IT security
+interfere with the platform's objectives. The protection shall
+correct operation. This includes be commensurate with the
+protection for the physical value of the IT assets protected
+infrastructure on which the by the TOE.
+TOE depends for correct
+operation and hardware
+devices on which the TOE is
+executing.
+Assumption Environmental Objective Rationale for Specifying the
+Addressing the Assumption Environmental Security
 Objective
-A.PHYSICAL OE.PHYSICAL OE.PHYSICAL
-The operational Those responsible for the TOE shall supports this assumption by
-environment is ensure that those parts of the TOE ensuring that the parts of the TOE
-assumed to critical to enforcement of the security critical to the enforcement of the
-provide the TOE policy are protected from physical attack security policy are protected
from
-with appropriate that might compromise IT security physical attack.
-physical objectives. The protection shall be
-protection such commensurate with the value of the IT
-that the TOE is assets protected by the TOE.
-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 OE.INFO_PROTECT OE.INFO_PROTECT
-and hardware
-Those responsible for the TOE shall supports the assumption by
-devices on which
-establish and implement procedures to requiring that all network and
-the TOE is
-ensure that information is protected in peripheral cabling must be
-executing.
-an appropriate manner. In particular: approved for the transmittal of the
-most sensitive data transmitted
-  All network and peripheral cabling
-over the link. Such physical links
```

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

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

```
-accomplish a task are trained to exercise control
-• All network and peripheral cabling
-or group of tasks over their own data.
-shall be approved for the transmittal
-within a secure IT
-of the most sensitive data
-environment by
+OE.INFO_PROTECT Those OE.INFO_PROTECT supports the
+responsible for the TOE shall policy by ensuring that users
+establish and implement are authorized to access parts
+procedures to ensure that of the data managed by the
+information is protected in an TOE.
+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
-exercising control
-physical links are assumed to be
-over their user
-adequately protected against threats
-data.
-to the confidentiality and integrity of
-the data transmitted using
-appropriate physical and logical
-protection techniques.
-• DAC protections on security-relevant
-files (such as audit trails and
-authentication databases) shall
-always be set up correctly.
-• Users are authorized to access parts
-of the data managed by the TOE
-and are trained to exercise control
+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.
-Assumption Environmental Objective Addressing Rationale for Specifying the
-the Assumption Environmental Security
+Assumption Environmental Objective Rationale for Specifying the
+Addressing the Assumption Environmental Security
 Objective
-P.USER OE.ADMIN OE.ADMIN
-Authority shall Those responsible for the TOE are supports the policy by ensuring
-only be given to competent and trustworthy individuals, that the authorized
administrators,
-users who are capable of managing the TOE and the responsible for granting authority
-trusted to perform security of information it contains. to users, are trustworthy.
-the actions
-correctly. OE.INFO_PROTECT OE.INFO_PROTECT
-Those responsible for the TOE shall supports the policy by ensuring
-establish and implement procedures to that users are authorized to
-ensure that information is protected in access parts of the data managed
-an appropriate manner. In particular: by the TOE.
- All network and peripheral cabling
-shall be approved for the transmittal
-of the most sensitive data
+T.UNAUTHORIZED + _ACCESS A OE.INFO_PROTECT Those OE.INFO_PROTECT diminishes
+user may gain unauthorized responsible for the TOE shall the logical and physical
threats
+access to user data for which establish and implement by ensuring that the network
+they are not authorized procedures to ensure that and peripheral cabling are
+according to the TOE security information is protected in an appropriately protected.
DAC
+policy. appropriate manner. In protections, when implemented
+particular: All network and correctly, support the
+peripheral cabling shall be identification of unauthorized
+approved for the transmittal of access.
+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
+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.
-T.UNAUTHORIZ OE.INFO_PROTECT OE.INFO_PROTECT
-ED
-Those responsible for the TOE shall diminishes the logical and
-_ACCESS establish and implement procedures to physical threats by ensuring that
-A user may gain ensure that information is protected in the network and peripheral
-unauthorized an appropriate manner. In particular: cabling are appropriately
-access to user protected.
-  All network and peripheral cabling
-data for which
-shall be approved for the transmittal DAC protections, when
-they are not of the most sensitive data implemented correctly, support
-authorized
-transmitted over the link. Such the identification of unauthorized
-according to the physical links are assumed to be access.
-TOE security
-adequately protected against threats
-policy.
-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
-Assumption Environmental Objective Addressing Rationale for Specifying the
-the Assumption Environmental Security
+8.4. Rationale for TOE Security Functional
+Requirements
+The following table provides the rationale for the selection of the security functional
requirements.
+It traces each TOE security objective to the identified security functional
requirements.
```

```
+Table 10. Table 10: Rationale for TOE Security Functional Requirements
+Objective Requirements Addressing the Rationale
 Objective
-of the data managed by the TOE
-and are trained to exercise control
-over their own data.
-C.4 Rationale for TOE Security Functional Requirements
-The following table provides the rationale for the selection of the security functional
-requirements. It traces each TOE security objective to the identified security
-functional requirements.
-Table 10: Rationale for TOE Security Functional Requirements
-Objective Requirements Rationale
-Addressing the
+O.ADMIN_ROLE The TOE shall FMT_SMR.1 The TOE will establish, at least,
+provide roles that allow only an authorized administrator
+authorized users to have access role and authorized user roles.
+to administrative privileges that Additional roles may also be
+are specific to the role. specified.
+Objective Requirements Addressing the Rationale
 Objective
-O.ADMIN_ROLE FMT_SMR.1 The TOE will establish, at
-The TOE shall provide roles that least, an authorized
-administrator role. Additional
-allow only authorized users to have
-access to administrative privileges roles may also be specified.
-that are specific to the role.
-Objective Requirements Rationale
-Addressing the
+O.AUDIT_GENERATION The TOE FAU_GEN.1 FAU_GEN.2 FAU_GEN.1 defines the set of
+shall provide the capability to FAU_SEL.1 events for which the TOE must
+detect and create records of be capable of generating audit
+security relevant events data. This requirement ensures
+associated with users. that the administrator has the
+ability to audit any security
+relevant events that takes place
+in the TOE. This requirement
+also defines the information
+that must be contained in the
+audit data for each auditable
+event. FAU_GEN.2 ensures that
+the audit data associates a user
+identity and, when applicable, a
+group identity with the
+auditable event. FAU_SEL.1
+allows the administrator to
+configure which auditable
+events will be recorded in the
+audit trail.
```

```
+O.DISCRETIONARY_ACCESS The FDP_ACC.1 FDP_ACF.1 The TSF controls access to
+TSF shall control access of resources based on the subject
+subjects and/or users to named and/or object security
+resources based on identity of attributes.
+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.
+Objective Requirements Addressing the Rationale
 Objective
-O.AUDIT_GENERATION FAU_GEN.1 FAU_GEN.1 defines the set
-The TOE shall provide the capability FAU_GEN.2 of events that the TOE must
-to detect and create records of be capable of recording.
-FAU_SEL.1
-security relevant events associated This requirement ensures
-with users. that the administrator has
-the ability to audit any
-security relevant events that
-takes place in the TOE. This
-requirement also defines the
-information that must be
-contained in the audit record
-for each auditable event.
-FAU_GEN.2 ensures that
-the audit records associate
-a user and any associated
-group identity with the
-auditable event.
-FAU_SEL.1 allows the
-administrator to configure
-which auditable events will
-be recorded in the audit trail.
-O.DISCRETIONARY_ACCESS FDP_ACC.1 The TSF controls access to
-resources based on the
-The TSF shall control access of FDP_ACF.1
-subject and/or object
-subjects and/or users to named
-security attributes.
-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 FIA_ATD.1 FIA_UID.2 and
-FIA_UAU.2ensure that only
-The TOE shall ensure that users are FIA_UAU.2
-authenticated before the TOE authorized users gain
-FIA_UID.2
-processes any actions that require access to the TOE and its
-FIA_USB_EXT.2
-resources following
-authentication.
-(Optional)
+O.I&A The TOE shall ensure that FIA_ATD.1 FIA_UAU.2 FIA_UID.2 FIA_UID.2 and FIA_UAU.2
+users are authenticated before FIA_USB_EXT.2 (Optional) ensure that only authorized
+the TOE processes any actions users gain access to the TOE
+that require authentication. and its resources following
 identification and
-authentication.
-FIA_ATD.1 ensures that the
-security attributes used to
-determine access are
-defined and available to the
-support access control
-decisions.
+authentication. FIA_ATD.1
+ensures that the security
+attributes used to determine
+access are defined and
+available to support access
+control decisions.
 FIA_USB_EXT.2 ensures
 enforcement of the rules
-governing subjects acting
-on behalf of authorized
-users.
-Objective Requirements Rationale
-Addressing the
+governing subjects acting on
+behalf of authorized users.
+O.MANAGE The TSF shall FMT_MSA.1(1) FMT_MSA.1(2) FMT_MSA.1(1) and
+provide all the functions and FMT_MSA.3 FMT_MTD.1 FMT_MSA.1(2) ensure that the
+facilities necessary to manage FMT_REV.1(1) FMT_REV.1(2) ability to perform operations
on
+TOE security mechanisms, and FMT_SMF.1 FMT_SMR.1 security attributes is restricted
+shall restrict such management to authorized administrators
+actions to authorized users. 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) and FMT_REV.1(2)
+restrict the ability to revoke
+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.
+Objective Requirements Addressing the Rationale
 Objective
-O.MANAGE FMT_MSA.1 FMT_MSA.1 ensures that
-The TSF shall provide all the FMT_MSA.3 the ability to perform
-functions and facilities necessary to operations on security
-FMT_MTD.1
-manage TOE security mechanisms, attributes is restricted to
-FMT_REV.1(1)
-and shall restrict such management authorized administrators.
-FMT_REV.1(2)
-actions to authorized users. FMT_MSA.3 ensures that
-FMT_SMF.1
-default values used for
-FMT_SMR.1 security attributes are
-restrictive.
-FMT_MTD.1 ensures that
-the ability to include or
-exclude auditable events is
-restricted to authorized
-administrators.
-FMT_REV.1 restricts the
-ability to revoke attributes to
-the authorized administrator.
-FMT_SMF.1 identifies the
-management functions that
-are available to the
-authorized administrator.
-FMT_SMR.1 defines the
-specific security roles to be
-supported.
 O.RESIDUAL_INFORMATION FDP_RIP.1 FDP_RIP.1 ensures that the
-contents of resources are
-The TOE shall ensure that any
-not available upon
-information contained in a protected
```

```
-reallocation of the resource.
-resource within its control is not
-inappropriately disclosed when the
-resource is reallocated.
-O.TOE_ACCESS FDP_ACC.1 FDP_ACC.1 and
-FDP_ACF.1 ensure that
-The TOE shall provide mechanisms FDP_ACF.1
-that control a user's logical access to access between subjects
-FIA_ATD.1
-and objects is controlled
-user data and to the TSF.
-FTA_MCS.1
-using security attributes.
-FTA_TSE.1
-FIA_ATD.1 defines the
-FTA_TAH_EXT.1 security attributes for
-(Optional) individual users.
-FPT_TRC.1 (Optional) FTA_MCS.1 ensures that
-users are restricted to no
-more than a specified
-number of concurrent
-sessions.
-FTA_TSE.1 allows the TOE
-to restrict access to the TOE
+The TOE shall ensure that any contents of resources are not
+information contained in a available upon reallocation of
+protected resource within its the resource.
+control is not inappropriately
+disclosed when the resource is
+reallocated.
+Objective Requirements Addressing the Rationale
+Objective
+O.TOE_ACCESS The TOE shall FDP_ACC.1 FDP_ACF.1 FDP_ACC.1 and FDP_ACF.1
+provide mechanisms that FIA_ATD.1 FTA_MCS_EXT.1 ensure that access between
+control a user's logical access to FTA_MCS.1 (Selection-Based) subjects and objects is
+user data and to the TSF. FTA_TSE.1 FTA_TAH_EXT.1 controlled using security
+(Optional) FPT_TRC.1 (Optional) attributes. FIA_ATD.1 defines
+the security attributes for
+individual users.
+FTA_MCS_EXT.1 ensures that
+the TOE restricts the maximum
+number of concurrent sessions
+using the mechanism selected
+by the ST author and allows the
+authorized administrator to
+configure the selected
+enforcement mechanism.
+FTA_MCS.1, when selected
```

```
+through 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.
-Objective Requirements Rationale
-Addressing the
-Objective
-FTA_TAH_EXT.1
-The TOE must be able to
-store and retrieve
+FTA_TAH_EXT.1 The TOE must
+be able to store and retrieve
 information about previous
 unauthorized login attempts
 and the number of times the
-login was attempted every
-time the user logs into their
-account. The TOE must also
-store the last successful
-authorized login. This
-information will include the
-date, time, method, and
-location of the attempts.
-Access to this data is
-controlled and restricted
-such that a user may only
-access his or her own data.
-FPT_TRC.1
-If included in an ST,
-FPT_TRC.1 ensures
-replicated TSF data that
-specifies attributes for
-access control must be
-consistent across distributed
-components of the TOE.
-The requirement is to
+login was attempted every time
+the user logs into their account.
+The TOE must also store the last
+successful authorized login.
+This information will include
+the date, time, method, and
+location of the attempts. Access
+to this data is controlled and
+restricted such that a user may
```

```
+only access his or her own data.
+FPT_TRC.1 If included in an ST,
+FPT_TRC.1 ensures replicated
+TSF data that specifies
+attributes for access control
+must be consistent across
+distributed components of the
+TOE. The requirement is to
 maintain consistency of
 replicated TSF data and
-associated access controls.
-C.5 SFR Dependencies Analysis
+associated access controls. 53
+8.5. SFR Dependencies Analysis
 Requirement Dependency Satisfied
-FAU_GEN.1 FPT_STM.1 This requirement is satisfied by the
-assumption on the IT environment, given in
+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.
-FIA_UID.1
-This requirement is satisfied by FIA_UID.2
-which is hierarchical to FIA_UID.1.
-FAU_SEL.1 FAU_GEN.1 This requirement is satisfied by
-FMT_MTD.1 FAU_GEN.1.
-This requirement is satisfied by
-FMT_MTD.1.
+FAU_GEN.2 FAU_GEN.1 FIA_UID.1 This requirement is satisfied by
+FAU_GEN.1. This requirement is
+satisfied by FIA_UID.2 which is
+hierarchical to FIA_UID.1.
+FAU_SEL.1 FAU_GEN.1 FMT_MTD.1 This requirement is satisfied by
+FAU_GEN.1. This requirement is
+satisfied by FMT_MTD.1.
 FDP_ACC.1 FDP_ACF.1 This requirement is satisfied by
 FDP_ACF.1.
-FDP_ACF.1 FDP_ACC.1 This requirement is satisfied by
-FDP_ACC.1.
-FMT_MSA.3
-This requirement is satisfied by
-FMT_MSA.3.
+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_UAU.2 FIA_UID.1 This requirement is satisfied by
+FIA_UID.2 which is hierarchical
+to FIA_UID.1.
 FIA_UID.2 None N/A
-FIA_USB_EXT.2 FIA_ATD.1 This requirement is satisfied by FIA_ATD.1.
-FMT_MSA.1 [FDP_ACC.1 or This requirement is satisfied by
-FDP_IFC.1] FDP_ACC.1.
-FMT_SMF.1 This requirement is satisfied by
-FMT_SMF.1.
-FMT_SMR.1
-This requirement is satisfied by
+FIA_USB_EXT.2 FIA_ATD.1 This requirement is satisfied by
+FIA_ATD.1.
+FMT_MSA.1(1) [FDP_ACC.1 or FDP_IFC.1] This requirement is satisfied by
+FMT_SMF.1 FMT_SMR.1 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 This requirement is satisfied by
-FMT_SMR.1 FMT_MSA.1.
-This requirement is satisfied by
+FMT_MSA.1(2) [FDP_ACC.1 or FDP_IFC.1] This requirement is satisfied by
+FMT_SMF.1 FMT_SMR.1 FDP_ACC.1. This requirement is
+satisfied by FMT_SMF.1. This
+requirement is satisfied by
 FMT_SMR.1.
-FMT_MTD.1 FMT_SMF.1 This requirement is satisfied by
-FMT_SMR.1 FMT_SMF.1.
-This requirement is satisfied by
+FMT_MSA.3 FMT_MSA.1 FMT_SMR.1 This requirement is satisfied by
+FMT_MSA.1(1) and
+FMT_MSA.1(2). This
+requirement is satisfied by
 FMT_SMR.1.
+Requirement Dependency Satisfied
+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
-Requirement Dependency Satisfied
 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 For a distributed TOE, the dependency is
-satisfied through the environmental
-assumption, A.CONNECT, that assures the
-confidentiality and integrity of the
-transmitted data.
-FTA_MCS.1 FIA_UID.1 This requirement is satisfied by FIA_UID.2
-which is hierarchical to FIA_UID.1.
+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 For a distributed TOE, the
+dependency is satisfied through
+the environmental assumption,
+A.CONNECT, that assures the
+confidentiality and integrity of
+the transmitted data.
+FTA_MCS_EXT.1 FIA_UID.2 This requirement is satisfied by
+FIA_UID.2.
+FTA_MCS.1 FIA_UID.1 When FTA_MCS.1 is selected
+through FTA_MCS_EXT.1, this
+requirement is satisfied by
+FIA_UID.2 which is hierarchical
+to FIA_UID.1.
 FTA_TSE.1 None N/A
-C.6 SAR Dependencies Analysis
-The dependencies for security assurance requirements are all fulfilled based on the
-following facts:
-  EAL2 is completely self-sufficient with all dependencies being fulfilled with the
-package of EAL2.
-  The security assurance requirement of ALC_FLR.3, which is in addition to
-EAL2, does not have any dependencies.
-C.7 Rationale for Satisfying all Security Assurance Requirements
-This collaborative Protection Profile (cPP) is developed for use by commercial DBMS
-security software developers. Since the cPP will be applied 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.
-C.8 Rationale for Extended Security Functional Requirements
-The table below presents a rationale for the inclusion of the extended functional
-security requirements found in this PP. Note that there are no extended security
-assurance requirements (SAR).
-Table 11: Rationale for Extended Security Functional Requirements
```

```
-Extended Identifier Rationale
-Requirement
-FIA_USB_EXT.2 Enhanced user- Security attributes may be associated with a user
-subject binding to further restrict access or provide additional
-privileges.
-FTA_TAH_EXT.1 TOE access The TOE may make information related to
-information attempts to establish a session available to
-users.
-Glossary
-The terms, definitions and abbreviations given [CC1] apply to this document.
-Additional terms, definitions and abbreviations applicable only within the DBMS cPP
-context are given below:
-Terms and Definitions
+8.6. SAR Dependencies Analysis
+The dependencies for security assurance requirements are all fulfilled based on the
following facts:
+EAL2 is completely self-sufficient with all dependencies being fulfilled with the
package of EAL2 as
+defined in [CC5].
+The security assurance requirement of ALC_FLR.3, which is in addition to EAL2, does not
have any
+dependencies.
+8.7. Rationale for Satisfying all Security Assurance
+Requirements
+This collaborative Protection Profile (cPP) is developed for use by commercial DBMS
security
+software developers. Since the cPP will be applied to commercial DBMS products that are
used
+internationally the EAL2 assurance package defined in [CC5] 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.
+8.8. Rationale for Extended Security Functional
+Requirements
+The table below presents a rationale for the inclusion of the extended functional
security
+requirements found in this PP. Note that there are no extended security assurance
requirements
+(SAR).
```

```
+Table 11. Table 11: Rationale for Extended Security Functional Requirements
+Extended Requirement Identifier Rationale
+FIA_USB_EXT.2 Enhanced user-subject binding Security attributes may be
+associated with a user to
+further restrict access or
+provide additional privileges.
+FTA_TAH_EXT.1 TOE access information The TOE may make information
+related to attempts to establish
+a session available to users.
+FTA_MCS_EXT.1 Configurable Session Limiting The TOE can enforce
+Mechanisms concurrent session limits using
+per-user session locking or
+another TSF-enforced
+mechanism selected by the ST
+author.
+Chapter 9. Selection-Based Requirements
+As indicated in the introduction to this cPP, the baseline requirements are contained in
the body of
+this cPP. Additional requirements appear here if certain selections are made in the
baseline
+requirements.
+9.1. Class: TOE access (FTA)
+9.1.1. Limitation on multiple concurrent sessions (FTA_MCS)
+FTA_MCS.1 Basic limitation on multiple concurrent sessions
+FTA_MCS.1.1
+The TSF shall restrict the maximum number of concurrent sessions that belong to the same
user.
+FTA_MCS.1.2
+The TSF shall enforce, by default, a limit of [assignment: default number] sessions per
user.
+Application Note 17: The ST author is reminded that CC Part 2 [CC2] allows that the
default number
+may be defined as a management function in FMT.
+Chapter 10. Glossary
+The terms, definitions and abbreviations given [CC1] apply to this document. Additional
terms,
+definitions and abbreviations applicable only within the DBMS cPP context are given
below:
+10.1. Terms and Definitions
 Term Meaning
-Access Interaction between an entity and an object that results in the
-flow or modification of data.
-Access Control Security service that controls the use of resources2 and the
-disclosure and modification of data.3
-Accountability Property that allows activities in an IT system to be traced to
-the entity responsible for the activity.
-Administrator A user who has been specifically granted the authority to
-manage some portion or the entire TOE and whose actions
```

```
-may affect the DAC. Administrators may possess special
-privileges that provide capabilities to override portions of the
-access control policy.
+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 and the disclosure and modification of
+data.
+Accountability Property that allows activities in an IT system to
+be traced to the entity responsible for the
+activity.
+Administrator A user who has been specifically granted the
+authority to manage some portion or the entire
+TOE and whose actions may affect the DAC.
+Administrators may possess special privileges
+that provide capabilities to override portions of
+the access control policy.
 Application An executable program.
-Assurance A measure of confidence that the security features of an IT
-system are sufficient to enforce its security policy.
-Attack An intentional act attempting to violate the security policy of an
-IT system.
+Assurance A measure of confidence that the security
+features of an IT system are sufficient to enforce
+its security policy.
+Attack An intentional act attempting to violate the
+security policy of an IT system.
 Authentication Security measure that verifies a claimed identity.
-Authorization Permission, granted by an entity authorized to do so, to
-perform functions and access data.
-Authorized Administrator The authorized person in contact with the Target of Evaluation
-who is responsible for maintaining its operational capability.
-Authorized User An authenticated user who may, in accordance with the
-access control policy, perform an operation.
-Availability Timely4, reliable access to IT resources.
+Authorization Permission, granted by an entity authorized to
+do so, to perform functions and access data.
+Authorized Administrator The authorized person in contact with the Target
+of Evaluation who is responsible for
+maintaining its operational capability.
+Authorized User An authenticated user who may, in accordance
+with the access control policy, perform an
+operation.
+Availability Timely, reliable access to IT resources.
 Compromise Violation of a security policy.
-Confidentiality A security policy pertaining to the disclosure of data.
-Database Management System A suite of programs that typically manage large structured
sets
```

```
-(DBMS) of persistent data, offering ad hoc query facilities to many
-users. They are widely used in business applications.
-Discretionary Access Control A means of restricting access to objects based on the
identity
-2 Hardware and software
-3 Stored or communicated
-4 According to a defined metric
+Confidentiality A security policy pertaining to the disclosure of
+data.
 Term Meaning
-(DAC) of subjects and/or groups to which they belong. Those
-controls are discretionary in the sense that a subject with
-certain access permission is capable of passing that
-permission (perhaps indirectly) on to any other subject.
-Entity A subject, object, user or another IT device, which interacts
-with TOE objects, data, or resources.
-External IT entity Any trusted Information Technology (IT) product or system,
-outside of the TOE, which may, in accordance with the access
-control policy, perform an operation.
-Group A group is a defined set. It is often used to describe a defined
-set of users.
-Identity A representation (e.g., a string) uniquely identifying an
-authorized user, which can either be the full or abbreviated
-name of that user or a pseudonym.
-Integrity A security policy pertaining to the corruption of data and TSF
-mechanisms.
-Named Object An object that exhibits all of the following characteristics:
-• The object may be used to transfer information between
-subjects of differing user and/or group identities within the
-TSF.
-• Subjects in the TOE must be able to require a specific
-instance of the object.
-• The name used to refer to a specific instance of the
-object must exist in a context that potentially allows
-subjects with different user and/or group identities to
+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.
+Entity A subject, object, user or another IT device,
+which interacts with TOE objects, data, or
+resources.
```

```
+External IT entity Any trusted Information Technology (IT)
+product or system, outside of the TOE, which
+may, in accordance with the access control
+policy, perform an operation.
+Group A group is a defined set. It is often used to
+describe a defined set of users.
+Identity A representation (e.g., a string) uniquely
+identifying an authorized user, which can either
+be the full or abbreviated name of that user or a
+pseudonym.
+Integrity A security policy pertaining to the corruption of
+data and TSF mechanisms.
+Named Object An object that exhibits all of the following
+characteristics: The object may be used to
+transfer information between subjects of
+differing user and/or group identities within the
+TSF. Subjects in the TOE must be able to require
+a specific instance of the object. The name used
+to refer to a specific instance of the object must
+exist in a context that potentially allows subjects
+with different user and/or group identities to
 require the same instance of the object.
-Object An entity that contains or receives information and upon which
-subjects perform operations.
-Platform The environment in which application software runs. The
-platform can be an operating system, an execution
-environment which runs atop an operating system, or some
-combination of these.
-Public Object An object for which the TSF unconditionally permits all entities
-"read" access. Only the TSF or authorized administrators may
-create, delete, or modify the public objects.
-Security attributes TSF data associated with subjects, objects, and users that are
-used for the enforcement of the DAC policy.
+Object An entity that contains or receives information
+and upon which subjects perform operations.
+Platform The environment in which application software
+runs. The platform can be an operating system,
+an execution environment which runs atop an
+operating system, or some combination of these.
+Term Meaning
+Public Object An object for which the TSF unconditionally
+permits all entities "read" access. Only the TSF
+or authorized administrators may create, delete,
+or modify the public objects.
+Security attributes TSF data associated with subjects, objects, and
+users that are used for the enforcement of the
+DAC policy.
 Subject An entity that causes operation to be performed.
```

```
-Threat Capabilities, intentions and attack methods of adversaries, or
-any circumstance or event, with the potential to violate the
+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.
-TOE resources Anything useable or consumable in the TOE.
-Unauthorized user A user who may obtain access only to system provided public
-Term Meaning
-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.
-Acronyms used in this cPP
+10.2. Acronyms used in this cPP
 Acronym Meaning
 ACL Access Control List
 CC Common Criteria
 COTS Commercial Off The Shelf
 DAC Discretionary Access Control
 DBMS Database Management System
-DBMS Database Management System collaborative Protection Profile
-cPP
+DBMS cPP Database Management System collaborative
+Protection Profile
 I&A Identification and Authentication
 IT Information Technology
 ITSEF IT Security Evaluation Facility
@@ -2039,6 +1822,7 @@
 SAR Security Assurance Requirement
 SFP Security Functional Policy
 SFR Security Functional Requirement
+Acronym Meaning
 SPD Security Problem Definition
 ST Security Target
 TOE Target of Evaluation
```