Microsoft SQL Server 2017 Database Engine Common Criteria Evaluation (EAL4+)

Security Target

SQL Server 2017 Team

Author:	Wolfgang Peter (Microsoft Corporation)
Version:	1.4
Date:	2019-11-15

Abstract

This document is the Security Target (ST) for the Common Criteria certification of the database engine of SQL Server 2017.

Keywords

CC, ST, Common Criteria, SQL, Security Target, DBMS, Database Management System

This page intentionally left blank

Table of Contents

List of Tables

Page

List of Figures

Page

1 ST Introduction

This chapter presents Security Target (ST) and TOE identification information and a general overview of the ST. A ST contains the information technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet stated requirements. A ST principally defines:

a) A security problem expressed as a set of assumptions about the security aspects of the environment, a list of threats that the TOE is intended to counter, and any known rules with which the TOE must comply (chapter 3, Security Problem Definition).

b) A set of security objectives and a set of security requirements to address the security problem (chapters 4 and 6, Security Objectives and IT Security Requirements, respectively).

c) The IT security functionality provided by the TOE that meets the set of requirements (chapter 7, TOE Summary Specification).

1.1 ST and TOE Reference

This chapter provides information needed to identify and control this ST and its Target of Evaluation (TOE).

ST Title:	SQL Server 2017 Database Engine Common Criteria Evaluation (EAL4+) Security Target
ST Version:	1.4
Date:	2019-11-15
Author:	Wolfgang Peter, Microsoft Corporation
Certification-ID:	BSI-DSZ-CC-1050
TOE Identification:	SQL Server 2017 Database Engine Enterprise Edition x64 (English) (and its related guidance documentation ([AGD] and [AGD_ADD]))
TOE Version:	14.0.3223.3
TOE Platform:	Windows Server 2012 R2 Update[1] (English) Standard Edition and Microsoft Windows Server 2016 (English) Standard Edition
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 as of April 2017, English version ([CC]).
Evaluation Assurance Level:	EAL4 augmented by ALC_FLR.2
PP Conformance:	DBMS Working Group Technical Community Protection Profile for Database Management Systems (DBMS PP) Base Package, Version 2.12, March 23rd, 2017 ([PP]) and DBMS Working Group Technical Community DBMS Protection Profile Extended Package - Access History (DBMS PP_EP_AH), Version 1.02, March 23rd, 2017 ([EP])
Keywords:	CC, ST, Common Criteria, SQL, Security Target, DBMS, Database Management System

[1] (i.e. including KB2919355)

1.2 TOE Overview

The TOE is the database engine of SQL Server 2017. SQL Server is a Database Management System (DBMS).

The TOE has been developed as the core of the DBMS to store data in a secure way.

The security functionality of the TOE comprises:

- Security Management
- Access Control
- Identification and Authentication
- Security Audit
- Session Handling

A summary of the TOE security functionality can be found in chapter 1.3.4. A more detailed description of the security functionality can be found in chapter 7, TOE Summary Specification.

Note that only the SQL Server 2017 database engine is addressed in this ST. Other related products of the SQL Server 2017 platform, such as Analysis Services, provide services that are useful but are not central to the enforcement of security policies. Hence, security evaluation is not directly applicable to those other products.

1.3 TOE Description

This chapter provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration. The main purpose of this chapter is to bind the TOE in physical and logical terms. The chapter starts with a description of the product type before it introduces the physical scope, the architecture and last but not least the logical scope of the TOE.

1.3.1 Product Type

The product type of the TOE described in this ST is a database management system (DBMS) with the capability to limit TOE access to authorized users, enforce Discretionary Access Controls on objects under the control of the database management system based on user and/or role authorizations, and to provide user accountability via audit of users' actions.

A DBMS is a computerized repository that stores information and allows authorized users to retrieve and update that information. A DBMS may be a single-user system, in which only one user may access the DBMS at a given time, or a multi-user system, in which many users may access the DBMS simultaneously.

The TOE which is described in this ST is the database engine and therefore part of SQL Server 2017. It provides a relational database engine providing mechanisms for Access Control, Identification and Authentication and Security Audit.

The SQL Server platform additionally includes the following tools which are not part of the TOE:

- SQL Server Replication: Data replication for distributed or mobile data processing applications and integration with heterogeneous systems
- Machine Learning Services: Machine learning functionality
- Full-Text and Semantic Extractions for Search: Search engine for database contents
- Data Quality Services: Data quality database objects
- PolyBaseQuery Service for External Data: Provides access to non-relational external data

- Analysis Services: Online analytical processing (OLAP) capabilities for the analysis of large and complex datasets.
- Reporting Services: A comprehensive solution for creating, managing, and delivering both traditional, paper-oriented reports and interactive, Web-based reports.
- Management tools: The SQL Server platform includes integrated management tools for database management and tuning as well as tight integration with tools such as Microsoft Operations Manager (MOM) and Microsoft Systems Management Server (SMS).
- Development tools: SQL Server offers integrated development tools for the database engine, data extraction, transformation, and loading (ETL), data mining, OLAP, and reporting that are tightly integrated with Microsoft Visual Studio to provide end-to-end application development capabilities.

The TOE itself only comprises the database engine of the SQL Server 2017 platform which provides the security functionality as required by this ST. Any additional tools of the SQL Server 2017 platform interact with the TOE as a standard SQL client. The scope and boundary of the TOE will be described in the next chapter.

1.3.2 Physical Scope and Boundary of the TOE

The TOE is the database engine of the SQL Server 2017 and its related guidance documentation. This engine is available in two different configurations (x86, x64). Only the x64 version is subject to this evaluation.

Further, SQL Server 2017 is available in different editions. Only the Enterprise Edition (EE) is subject to this evaluation.

The following figure shows the TOE (including its internal structure) and its immediate environment.

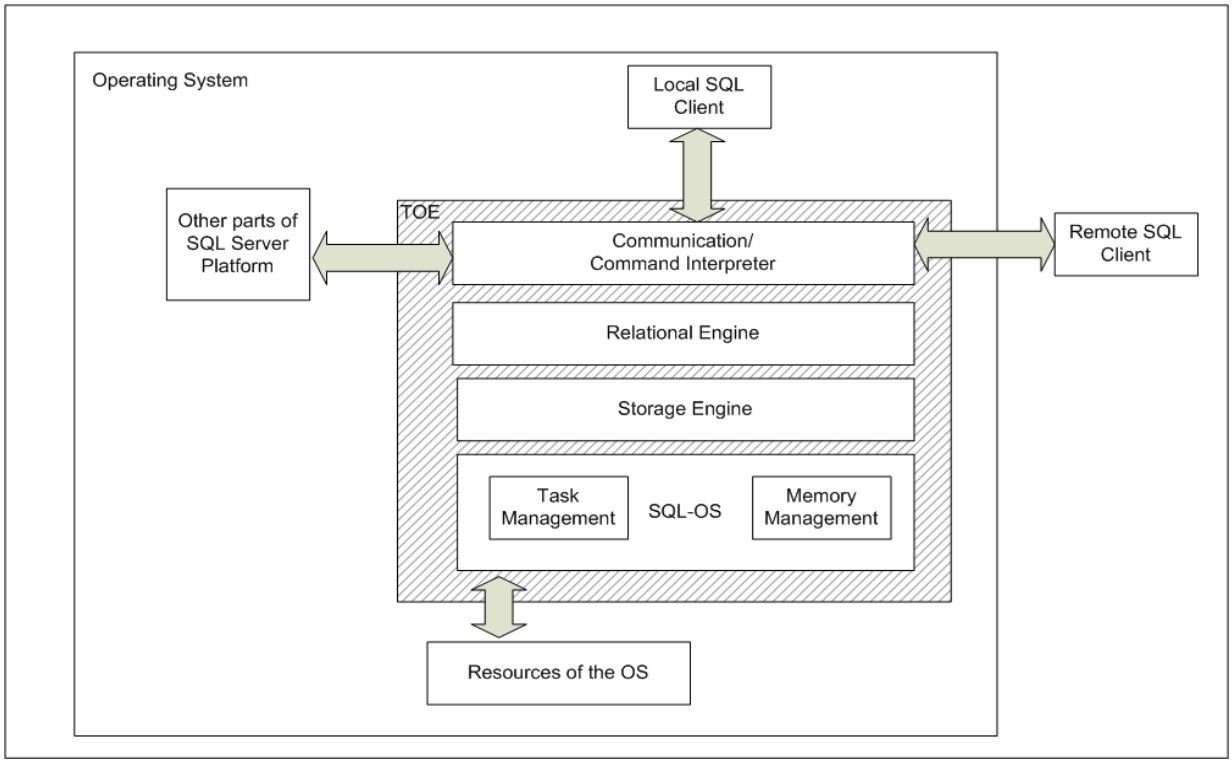

Figure 1 - TOE Structure

As seen in Figure 1 the TOE internally comprises the following units:

The **Communication** part is the interface for programs accessing the TOE. It is the interface between the TOE and clients performing requests.

All responses to user application requests return to the client through this part of the TOE.

The **Relational Engine** is the core of the database engine and is responsible for all security relevant decisions. The relational engine establishes a user context, syntactically checks every Transact SQL (T-SQL) statement, compiles every statement, checks permissions to determine if the statement can be executed by the user associated with the request, optimizes the query request, builds and caches a query plan, and executes the statement. The Relational Engine allows compiling a subset of T-SQL statements into native code to create natively compiled Stored Procedures. The Visual C compiler used for this native compilation is not part of the TOE.

The **Storage Engine** is a resource provider. When the relational engine attempts to execute a T-SQL statement that accesses an object for the first time, it calls upon the storage engine to retrieve the object, put it into memory and return a pointer to the execution engine. To perform these tasks, the storage engine manages the physical resources for the TOE by using the Windows OS.

The **SQL-OS** is a resource provider for all situations where the TOE uses functionality of the operating system. SQL-OS provides an abstraction layer over common OS functions and was designed to reduce the number of context switches within the TOE. SQL-OS especially contains functionality for Task Management and for Memory Management.

For **Task Management** the TOE provides an OS-like environment for threads, including scheduling, and synchronization - all running in user mode, all (except for I/O) without calling the Windows Operating System.

The **Memory Management** is responsible for the TOE memory pool. The memory pool is used to supply the TOE with its memory while it is executing. Almost all data structures that use memory in the TOE are allocated in the memory pool. The memory pool also provides resources for transaction logging and data buffers.

The immediate **environment** of the TOE comprises:

The Windows Server Operating System hosts the TOE. As the TOE is software only it lives as a process in the Operating System (OS) and uses the resources of the OS. These resources comprise general functionality (e.g. the memory management and scheduling features of the OS) as well as specific functionality of the OS, which is important for the security functionality of the TOE (see chapter 7 for more details).

Other parts of the SQL Server 2017 Platform might be installed together with the TOE. The TOE is the central part of a complete DBMS platform, which realizes all security functionality as described in this ST. However other parts of the platform may be installed on the same machine if they are needed to support the operation or administration of the TOE. However these other parts will interact with the TOE in the same way, every other client would do.

Clients (comprising local clients and remote clients) are used to interact with the TOE during administration and operation. Services of the Operating System are used to route the communication of remote clients with the TOE.

The TOE relies on functionality of the Operating System and has the following hardware/software requirements:

Table 1 - Hardware and Software Requirements

Aspect	Requirement
CPU	AMD Opteron, AMD Athlon 64, Intel Xeon with Intel EM64T support, Intel Pentium IV with EM64T support at 1.4 GHz or faster

Aspect	Requirement
RAM	1 GB
Hard Disk	Approx. 6 GB of free space
Other	DVD drive, display at Super VGA or higher resolution, Microsoft mouse compatible pointing device, keyboard
OS	Windows Server 2012 R2 (English), Standard Edition Windows Server 2016, Standard Edition
Software	.NET Framework 3.5 SP1

The TOE is downloadable as a DVD image via the Microsoft volume licensing service center (https://www.microsoft.com/licensing/servicecenter/default.aspx).

The following guidance documents and supportive information belong to the TOE:

- SQL Server Technical Documentation: This is the general guidance documentation for the complete SQL Server 2017 platform ([AGD]).
- SQL Server Guidance Addendum: This document contains the aspects of the guidance that are specific to the evaluated configuration of SQL Server 2017 ([AGD_ADD]).

The website https://www.microsoft.com/en-us/sql-server/data-security (click on “View our Common Criteria certification”) contains additional information about the TOE and its evaluated configuration. Also the guidance addendum that describes the specific aspects of the certified version can be obtained via this website. The guidance addendum extends the general guidance of SQL Server 2017.

This website shall be visited before using the TOE.

1.3.3 Architecture of the TOE

The TOE which is described in this ST comprises one instance of the SQL Server 2017 database engine but has the possibility to serve several clients simultaneously.

1.3.4 Logical Scope and Boundary of the TOE

SQL Server 2017 is able to run multiple instances of the database engine on one machine. After installation one default instance exists. However the administrator is able to add more instances of SQL Server 2017 to the same machine.

The TOE comprises one instance of SQL Server 2017. Within this ST it is referenced either as "the TOE" or as "instance". The machine the instances are running on is referenced as "server" or "DBMS-server".

If more than one instance of SQL Server 2017 is installed on one machine these just represent multiple TOEs as there is no other interface between two instances of the TOE than the standard client interface.

In this way two or more instances of the TOE may only communicate through the standard client interface.

The TOE provides the following set of security functionality:

- The **Access Control** function of the TOE controls the access of users to user and metadata stored in the TOE. It further controls that only authorized administrators are able to manage the TOE.
- The **Security Audit** function of the TOE produces log files about all security relevant events.

- The **Security Management** function allows authorized administrators to manage the behavior of the security functionality of the TOE.
- The **Identification and Authentication**[2] function of the TOE is able to identify and authenticate users.
- The **Session Handling** mechanism which limits the possibilities of users to establish sessions with the TOE and maintains a separate execution context for every operation. Also the Memory Management functionality belongs to the area of Session Handling and ensures that any previous information in memory is made unavailable before the memory is used either by overwriting the memory explicitly with a certain pattern or by overwriting the memory completely with new information.

The following functions are part of the environment:

- The **Audit Review** and **Audit Storage** functionality has to be provided by the environment and provide the authorized administrators with the capability to review the security relevant events of the TOE.
- The **Access Control Mechanisms** has to be provided by the environment for files stored in the environment.
- The environment provides **Identification and Authentication**[2] for users for the cases where this is required by the TOE (The environment AND the TOE provide mechanisms for user authentication. See chapter 7.3 for more details).
- The environment has to provide **Time stamps** to be used by the TOE.
- The environment provides a **cryptographic** mechanism for **hashing** of passwords.
- The environment provides **residual information protection** for memory which is allocated to the TOE.

All these functions are provided by the underlying Operating System except Audit Review. An additional tool (e.g. the SQL Server Profiler, which is part of the SQL Server Platform) has to be used for Audit Review.

Access to the complete functionality of the TOE is possible via a set of SQL-commands.

This set of commands is available via:

- Shared Memory
- Named Pipes
- TCP/IP

1.4 Conventions

For this Security Target the following conventions are used:

The CC allows several operations to be performed on functional requirements: *refinement*, *selection*, *assignment*, and *iteration* are defined in chapter C.4 of Part 1 of [CC]. Each of these operations is used in this ST.

A **refinement** operation (denoted by ~~**bold crossed out text**~~) is used to remove unnecessary details of a requirement, though it does not change the meaning of the requirement.

[2] Note that the TOE as well as the environment provides a mechanism for identification and authentication. Chapter 7 will describe this in more detail.

Moreover, a refinement operation (denoted by **bold text**) is used to add details to a requirement, and thus further restricts a requirement.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made are denoted by italicized text.

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 are denoted by showing the value in square brackets, [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 security target authors to create their own requirements. Such requirements are termed ‘extended requirements’ and are permitted if the CC does not offer suitable requirements to meet the authors’ needs. Extended requirements must be identified and are required to use the CC class/family/component model in articulating the requirements. In this ST, extended requirements will be indicated with the “EXT” following the component name.

2 Conformance Claims

2.1 CC Conformance Claim

This Security Target claims to be

- **CC Part 2 (Version 3.1, Revision 5, April 2017) extended** due to the use of the components FIA_USB_(EXT).2 and FTA_TAH_(EXT).1
- **CC Part 3 (Version 3.1, Revision 5, April 2017) conformant** as only assurance components as defined in part III of [CC] have been used.

Further this Security Target claims to be conformant to the Security Assurance Requirements package EAL 4 augmented by ALC_FLR.2.

2.2 PP Conformance Claim

This Security Target claims to be conformant to:

- DBMS Working Group Technical Community Protection Profile for Database Management Systems (DBMS PP) Base Package, Version 2.12, March 23rd, 2017 ([PP]), and
- DBMS Working Group Technical Community DBMS Protection Profile Extended Package - Access History (DBMS PP_EP_AH), Version 1.02, March 23rd, 2017 ([EP])

Though [PP] allows a demonstrable conformance this Security Target claims strict conformance to [PP].

The product type of the TOE (see section 1.3.1) is consistent with the product type of the TOE specified in [PP] (both are database management systems (DBMS)). As strict conformance to [PP] is claimed no further conformance claim rationale is required.

3 Security Problem Definition

This chapter describes

- the external entities interacting with the TOE,
- the assets that have to be protected by the TOE,
- assumptions about the environment of the TOE,
- threats against those assets, and
- organizational security policies that TOE shall comply with.

3.1 Assets

The following external entities interact with the TOE:

- Administrator:
  The administrator is authorized to perform the administrative operations and able to use the administrative functions.

- User:
  A person who wants to use the TOE.

- Attacker:
  An attacker is any individual who is attempting to subvert the operation of the TOE. The intention may be to gain unauthorized access to the assets protected by the TOE.

The TOE maintains two types of data which represent the assets: User Data and TSF Data.

The primary assets are the User Data which comprises 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
- User-developed queries or procedures that the DBMS maintains for users.

The secondary assets comprise the TSF data that the TOE maintains and uses for its own operation. It specifically includes:

- Configuration parameters,
- User security attributes,
- Security Audit instructions and records.

3.2 Assumptions

The following table lists all the assumptions about the environment of the TOE. These assumptions have been directly taken from [PP] without any modification.

Table 2 – Assumptions

Assumption	Description
Physical aspects	
A.PHYSICAL	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the

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

3.3 Threats

The following table identifies the threats to the TOE. These threats have been directly taken from [PP] without any modifications.

Table 3 – Threats to the TOE

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

3.4 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This chapter identifies the organizational security policies applicable to the TOE. These organizational security policies have been taken from [PP] without any changes.

Table 4 – Organizational Security Policies

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

4 Security Objectives

The purpose of the security objectives is to detail the planned response to a security problem or threat. This chapter describes the security objectives for the TOE and its operational environment.

4.1 Security Objectives for the TOE

This chapter identifies and describes the security objectives of the TOE. The objectives have been directly taken from [PP] with the exception of O.ACCESS_HISTORY which has been taken from [EP].

Table 5 – Security Objectives for the TOE

Objective	Description
O.ACCESS_HISTORY	The TOE will store information related to previous attempts to establish a session and make that information available to the user.
O.ADMIN_ROLE	The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.
O.AUDIT_GENERATION	The TSF must be able to record defined security-relevant events (which usually include security-critical actions of users of the TOE). The information recorded for security-relevant events must contain the time and date the event happened and, if possible, the identification of the user that caused the event, and must be in sufficient detail to help the authorized user detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.
O.DISCRETIONARY_ACCESS	The TSF must control access of subjects and/or users to named resources based on identity of the object, subject, or user. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.
O.I&A	The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.
O.MANAGE	The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.
O.MEDIATE	The TOE must protect user data in accordance with its security policy, and must mediate all requests to access

Objective	Description
	such data.
O.RESIDUAL_INFORMATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.
O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access[3] to user data and to the TSF.

4.2 Security Objectives for the operational Environment

The security objectives for the TOE Environment are defined in the following table. The objectives for the environment have been directly taken from [PP] without any changes.

Table 6 – Security Objectives for the TOE Environment

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

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

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

4.3 Security Objectives Rationale

4.3.1 Overview

The following table maps the security objectives to assumptions / threats / OSPs:

Threats, Assumptions, OSP / Security Objectives	O.ACCESS_HISTORY	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.DISCRETIONARY_ACCESS	O.I&A	O.MANAGE	O.MEDIATE	O.RESIDUAL_INFORMATION	O.TOE_ACCESS	OE.ADMIN	OE.INFO_PROTECT	OE.IT_I&A	OE.IT_REMOTE	OE.IT_TRUSTED_SYSTEM	OE.NO_GENERAL_ PURPOSE	OE.PHYSICAL
T.ACCESS_TSFDATA	X				X	X		X	X							
T.ACCESS_TSFFUNC		X			X	X		X	X							
T.IA_MASQUERADE	X				X		X		X						X	
T.IA_USER				X	X		X		X							
T.RESIDUAL_DATA								X								
T.TSF_COMPROMISE	X		X						X		X		X	X	X	X
T.UNAUTHORIZED_ACCESS				X		X	X				X					
P.ACCOUNTABILITY		X	X		X				X	X	X					
P.ROLES		X							X	X						
P.USER						X			X	X	X					
A.PHYSICAL											X					X
A.AUTHUSER											X		X	X		
A.MANAGE										X	X					
A.TRAINEDUSER											X					
A.NO_GENERAL_PURPOSE															X	
A.PEER_FUNC_&_MGT													X	X		
A.SUPPORT												X				
A.CONNECT											X		X	X		X

Table 7 – Summary of Security Objectives Rationale

Details are given in the following table. These details are directly taken from [PP] and [EP].

4.3.2 Rationale for TOE Security Objectives

Table 8 – Rationale for TOE Security Objectives

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE.	O.ADMIN_ROLE The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.	O.ADMIN_ROLE supports this policy by ensuring that the TOE has an objective to provide authorized administrators with the privileges needed for secure administration.
	O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security relevant events associated with users.	O.AUDIT_GENERATION supports this policy by ensuring that audit records are generated. Having these records available enables accountability.
	O.I&A The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.	O.I&A supports this policy by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE is defined to provide to authenticated users only.
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	O.TOE_ACCESS supports this policy by providing a mechanism for controlling access to authorized users.
P.USER Authority shall only be given to users who are trusted to perform the actions correctly.	O.MANAGE The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.	O.MANAGE supports this policy by ensuring that the functions and facilities supporting the authorized administrator role are in place.

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	O.TOE_ACCESS supports this policy by providing a mechanism for controlling access to authorized users.
	OE.ADMIN Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of information it contains.	OE.ADMIN supports this policy by ensuring that the authorized administrator role is understood and used by competent administrators.
P.ROLES Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible supporting only the administrative duties the person has. This role	O.ADMIN_ROLE The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.	O.ADMIN_ROLE The TOE has the objective of providing an authorized administrator role for secure administration. The TOE may provide other roles as well, but only the role of authorized administrator is required.
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	O.TOE_ACCESS supports this policy by ensuring that an authorized administrator role can be distinguished from other authorized users.
T.ACCESS_TSFDATA A threat agent may read or modify TSF data using functions of the TOE without the proper authorization.	O.ACCESS_HISTORY The TOE will store information related to previous attempts to establish a session and make that information available to the user.	O.ACCESS_HISTORY diminishes this threat because it ensures the TOE will store the information that is needed to advise the user of previous authentication attempts and allows this information to be retrieved.
	O.I&A The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.	O.I&A supports this policy by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE is defined to provide to authenticated users only.

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

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
	O.MANAGE The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.	O.MANAGE diminishes this threat because an access control policy is specified to control access to TSF data. This objective is used to dictate who is able to view and modify TSF data, as well as the behavior of TSF functions.
	O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.	O.RESIDUAL_INFORMATION diminishes this threat by ensuring that TSF data and user data is not persistent when resources are released by one user/process and allocated to another user/process.
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	O.TOE_ACCESS diminishes this threat since it makes it more unlikely that a threat agent has access to the TOE.
T.IA_MASQUERADE A user or process may masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources.	O.ACCESS_HISTORY The TOE will store information related to previous attempts to establish a session and make that information available to the user.	O.ACCESS_HISTORY diminishes this threat because it ensures the TOE will be able to store and retrieve the information that will advise the user of the last successful login attempt and performed actions without their knowledge.
	O.I&A The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.	O.I&A diminishes this threat by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE has defined to provide to authenticated users only

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
	O.MEDIATE The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.	O.MEDIATE diminishes this threat by ensuring that all access to user data are subject to mediation, unless said data has been specifically identified as public data. The TOE requires successful authentication to the TOE prior to gaining access to any controlled-access content. By implementing strong authentication to gain access to these services, an attacker's opportunity to masquerade as another entity in order to gain unauthorized access to data or TOE resources is reduced.
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	O.TOE_ACCESS diminishes this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanism this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE.
T.IA_USER A threat agent may gain access to user data, TSF data or TOE resources with the exception of	O.DISCRETIONARY_ACCESS The TSF must control access of subjects and/or users to named resources based on identity of the object, subject, or user. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.	O.DISCRETIONARY_ACCESS diminishes this threat by requiring that data including user data stored with the TOE, have discretionary access control protection.

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
	O.I&A The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.	O.I&A diminishes this threat by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE is defined to provide to authenticated users only.
	O.MEDIATE The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.	O.MEDIATE diminishes this threat by ensuring that all access to user data are subject to mediation, unless said data has been specifically identified as public data. The TOE requires successful authentication to the TOE prior to gaining access to any controlled-access content. By implementing strong authentication to gain access to these services, an attacker's opportunity to masquerade as another entity in order to gain unauthorized access to data or TOE resources is reduced.
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	O.TOE_ACCESS diminishes this threat by controlling logical access to user data, TSF data or TOE resources.
T.RESIDUAL_DATA A user or process may gain unauthorized access to user or TSF data through reallocation of	O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.	O.RESIDUAL_INFORMATION diminishes this threat because even if the security mechanisms do not allow a user to view TSF data, if TSF data were to reside inappropriately in a resource that was made available to a user, that user would be able to view the TSF data without authorization.

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
T.TSF_COMPROMISE A malicious user or process may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable code within the TSF.	O.ACCESS_HISTORY The TOE will store information related to previous attempts to establish a session and make that information available to the user.	O.ACCESS_HISTORY diminishes this threat because it ensures the TOE will be able to store and retrieve the information that will advise the user of the last successful login attempt and performed actions without their knowledge.
	O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security relevant events associated with users.	O.AUDIT_GENERATION diminishes this threat by providing the authorized administrator with the appropriate audit records supporting the detection of compromise of the TSF.
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	O.TOE_ACCESS diminishes this threat since controlled user's logical access to the TOE will reduce the opportunities for an attacker’s access to configuration data.
T.UNAUTHORIZED_ACCESS A user may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.	O.DISCRETIONARY_ACCESS The TSF must control access of subjects and/or users to named resources based on identity of the object, subject or user. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.	O.DISCRETIONARY_ACCESS diminishes this threat by requiring that data including TSF data stored with the TOE, have discretionary access control protection.
	O.MANAGE The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.	O.MANAGE diminishes this threat by ensuring that the functions and facilities supporting that authorized users can be held accountable for their actions by authorized administrators are in place.

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
	O.MEDIATE The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.	O.MEDIATE diminishes this threat because it ensures that all access to user data are subject to mediation, unless said data has been specifically identified as public data. The TOE requires successful authentication to the TOE prior to gaining access to any controlled-access content. By implementing strong authentication to gain access to these services, an attacker's opportunity to conduct a man-in-the-middle and/or password guessing attack successfully is greatly reduced. Lastly, the TSF will ensure that all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services. The TOE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc. to the administrator. This feature ensures that no other user can modify the information flow policy to bypass the intended TOE security policy.

4.3.3 Rationale for Environmental Security Objectives

The following table contains the rationale for the IT Environmental Objectives. This rationale has directly been taken from [PP] without any changes.

Table 9 – Rationale for IT Environmental Objectives

Assumption	Environmental Objective Addressing the Assumption	Rationale
A.AUTHUSER Authorized users possess the necessary authorization to access at least some of the	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an	OE.INFO_PROTECT supports the assumption by ensuring that users are authorized to access parts of the data managed by the TOE

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

Assumption	Environmental Objective Addressing the Assumption	Rationale
	are managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.	
A.CONNECT All connections to and from remote trusted IT systems and between separate parts of the TSF are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.	OE.IT_REMOTE If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions, required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.	OE.IT_REMOTE supports the assumption by levying a requirement in the environment that connections between trusted systems or physically separated parts of the TOE are sufficiently protected from any attack that may cause those functions to provide false results.
	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data	OE.INFO_PROTECT supports the assumption by requiring that All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques

Assumption	Environmental Objective Addressing the Assumption	Rationale
	managed by the TOE and are trained to exercise control over their own data.	
	OE.IT_TRUSTED_SYSTEM The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.	OE.IT_TRUSTED_SYSTEM supports the assumption by ensuring that remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy.
	OE.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.	OE.PHYSICAL supports the assumption by ensuring that appropriate physical security is provided within the domain.
A.SUPPORT Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is used by the TOE is correct and up to date.	OE.IT_I&A Any information provided by a trusted entity in the environment and used to support user authentication and authorization used by the TOE is correct and up to date.	OE.IT_I&A supports the assumption implicitly.
A.MANAGE The TOE security functionality is managed by one or more competent individuals. The system administrative personnel are not careless, willfully	OE.ADMIN Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of information it	OE.ADMIN supports the assumption since the authorized administrators are assumed competent in order to help ensure that all the tasks and responsibilities are performed

Assumption	Environmental Objective Addressing the Assumption	Rationale
negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.	contains.	effectively.
	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT supports the assumption by ensuring that the information protection aspects of the TOE and the system(s) and relevant connectivity that form the platform for the TOE is vital to addressing the security problem, described in this PP. Managing these effectively using defined procedures is reliant on having competent administrators.
A.NO_GENERAL_PURPOSE There are no general-purpose computing or storage repository capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration, and support of the DBMS.	OE.NO_GENERAL_PURPOSE There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on DMBS servers, other than those services necessary for the operation, administration, and support of the DBMS.	OE.NO_GENERAL_PURPOSE The DBMS server must not include any general-purpose computing or storage capabilities. This will protect the TSF data from malicious processes. The environmental objective is tightly related to the assumption, which when fulfilled will address the assumption.

Assumption	Environmental Objective Addressing the Assumption	Rationale
A.PEER_FUNC_&_MGT All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.	OE.IT_REMOTE If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions, required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.	OE.IT_REMOTE The assumption that connections between trusted systems or physically separated parts of the TOE is addressed by the objective specifying that such systems are sufficiently protected from any attack that may cause those functions to provide false results.
	OE.IT_TRUSTED_SYSTEM The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.	OE.IT_TRUSTED_SYSTEM The assumption on all remote trusted IT systems to implement correctly the functionality used by the TSF consistent with the assumptions defined for this functionality is supported by physical and logical protections and the application of trusted policies commensurate with those applied to the TOE.
A.PHYSICAL It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.	OE.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.	OE.PHYSICAL The TOE, the TSF data, and protected user data is assumed to be protected from physical attack (e.g., theft, modification, destruction, or eavesdropping). Physical attack could include unauthorized intruders into the TOE environment, but it does not include physical destructive actions that might be taken by an individual that is authorized to access the TOE environment.
	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that	OE.INFO_PROTECT supports the assumption by ensuring that users are authorized to access parts of the

Assumption	Environmental Objective Addressing the Assumption	Rationale
	information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	data managed by the TOE and is trained to exercise control over their own data.
A.TRAINEDUSER Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection	OE.INFO_PROTECT supports the assumption by requiring that all network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques.

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

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

Assumption	Environmental Objective Addressing the Assumption	Rationale
	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.IA_MASQUERADE A user or process may masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources.	OE.NO_GENERAL_PURPOSE There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on DMBS servers, other than those services necessary for the operation, administration, and support of the DBMS.	OE.NO_GENERAL_PURPOSE The DBMS server must not include any general-purpose computing or storage capabilities. This diminishes the threat of masquerade since only users with DBMS or related functions will be defined in the TOE environment.
T.TSF_COMPROMISE A malicious user or process may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable code within the TSF.	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise	OE.INFO_PROTECT supports the policy by ensuring that users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data and that DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly.

Assumption	Environmental Objective Addressing the Assumption	Rationale
	control over their own data.	
	OE.IT_REMOTE If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions, required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.	OE.IT_REMOTE diminishes the threat by ensuring that remote trusted IT systems are sufficiently protected.
	OE.IT_TRUSTED_SYSTEM The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.	OE.IT_TRUSTED_SYSTEM diminishes the threat by ensuring that remote trusted IT systems are managed according to known, accepted and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.
	OE.NO_GENERAL_PURPOSE There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on DMBS servers, other than those services necessary for the operation, administration, and support of the DBMS	OE.NO_GENERAL_PURPOSE diminishes this threat by reducing the opportunities to subvert non TOE related capabilities in the TOE environment.
	OE.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must	OE.PHYSICAL diminishes the threat of a TSF compromise due to exploitation of physical weaknesses or vulnerabilities as a vector in an attack.

Assumption	Environmental Objective Addressing the Assumption	Rationale
	be commensurate with the value of the IT assets protected by the TOE.	
T.UNAUTHORIZED_ACCESS A user may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT diminishes the threat by ensuring that the logical and physical threats to network and peripheral cabling are appropriately protected. DAC protections if implemented correctly may support the identification of unauthorized accesses.

5 Extended Components Definitions

5.1 Definition for FTA_TAH_(EXT).1

This chapter defines the extended functional component FTA_TAH_(EXT).1 TOE access information. The definition has been directly taken from [EP].

FTA_TAH_(EXT).1 TOE access information provides the requirement for a TOE to make available information related to attempts to establish a session.

Component levelling

FTA_TAH_(EXT).1 is not hierarchical to any other components.

Management: FTA_TAH_(EXT).1

There are no management activities foreseen.

Audit: FTA_TAH_(EXT).1

There are no auditable events foreseen.

FTA_TAH_(EXT).1 TOE access information

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

FTA_TAH_(EXT).1.1

Upon a session establishment attempt, the TSF shall store

a. the [date and time] of the session establishment attempt of the user.

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

FTA_TAH_(EXT).1.2

Upon successful session establishment, the TSF shall allow the [date and time] of

a. the previous last successful session establishment, and

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

to be retrieved by the user.

5.2 Definition for FIA_USB_(EXT).2

This chapter defines the extended functional component FIA_USB_(EXT).2 Enhanced user-subject binding. The definition has been directly taken from [PP].

FIA_USB_(EXT).2 is analogous to FIA_USB.1 except that it adds the possibility to specify rules whereby subject security attributes are also derived from TSF data other than user security attributes.

Component leveling

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

Management

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

Audit

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

FIA_USB_(EXT).2 Enhanced user-subject binding

Hierarchical to: FIA_USB.1 User-subject binding

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB_(EXT).2 .1

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

FIA_USB_(EXT).2 .2

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

FIA_USB_(EXT).2 .3

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

FIA_USB_(EXT).2 .4

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

6 IT Security Requirements

This chapter defines the IT security requirements that shall be satisfied by the TOE or its environment:

Common Criteria divides TOE security requirements into two categories:

- Security functional requirements (SFRs) (such as, identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.
- Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g., configuration management, testing, and vulnerability assessment).

These requirements are discussed separately within the following subchapters.

6.1 TOE Security Functional Requirements

The TOE satisfies the SFRs delineated in the following table. The rest of this chapter contains a description of each component and any related dependencies.

Table 10 – TOE Security Functional Requirements

Class FAU: Security Audit	
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SEL.1	Selective audit
Class FDP: User Data Protection	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_RIP.1	Subset residual information protection
Class FIA: Identification and Authentication	
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FIA_USB_(EXT).2	Enhanced user subject binding
Class FMT: Security Management	
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data
FMT_REV.1(1)	Revocation (user attributes)
FMT_REV.1(2)	Revocation (subject, object attributes)
FMT_SMF.1	Specification of management functions

FMT_SMR.1	Security roles
Class FPT: Protection of the TSF	
FPT_TRC.1	Internal TSF consistency
Class FTA: TOE Access	
FTA_MCS.1	Basic limitation on multiple concurrent sessions
FTA_TAH_(EXT).1	TOE access information
FTA_TSE.1	TOE session establishment

6.1.1 Class FAU: Security Audit

Audit data generation (FAU_GEN.1)

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 11;** and
c) [Start-up and shutdown of the DBMS;
d) Use of special permissions (e.g., those often used by authorized administrators to circumvent access control policies); and
e) *no additional events*].

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of Table 11, below].

Table 11 – Auditable Events

Security Functional Requirement	Auditable Event(s)	Additional Audit Record Contents
FAU_GEN.1	None	None
FAU_GEN.2	None	None
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	The identity of the authorized administrator that made the change to the audit configuration
FDP_ACC.1	None	None
FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP.	The identity of the subject performing the operation
FDP_RIP.1	None	None
FIA_ATD.1	None	None

Security Functional Requirement	Auditable Event(s)	Additional Audit Record Contents
FIA_UAU.1	Unsuccessful use of the authentication mechanism	None
FIA_UID.1	Unsuccessful use of the user identification mechanism, including the user identity provided	None
FIA_USB_(EXT).2	Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject)	None
FMT_MOF.1	None	None
FMT_MSA.1	None	None
FMT_MSA.3	None	None
FMT_MTD.1	None	None
FMT_REV.1(1)	Unsuccessful revocation of security attributes.	Identity of individual attempting to revoke security attributes
FMT_REV.1(2)	Unsuccessful revocation of security attributes.	Identity of individual attempting to revoke security attributes
FMT_SMF.1	Use of the management functions.	Identity of the administrator performing these functions
FMT_SMR.1	Modifications to the group of users that are part of a role.	Identity of authorized administrator modifying the role definition
FTA_MCS.1	Rejection of a new session based on the limitation of multiple concurrent sessions	None
FTA_TAH_(EXT).1	None	None
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism	Identity of the individual attempting to establish a session

User identity association (FAU_GEN.2)

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

Selective audit (FAU_SEL.1)

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

a) object identity;

b) user identity;

c) ***no other identities***;

d) event type;

e) [success of auditable security events;

f) failure of auditable security events; and

g) [*no additional criteria*].]

Application Note: ([PP, 7.1.1.3]) The intent of this requirement is to capture enough audit data to allow the administrators to perform their task, not necessarily to capture only the needed audit data. In other words, the DBMS does not necessarily need to include or exclude auditable events based on all attributes at any given time.

6.1.2 Class FDP: User Data Protection

Subset access control (FDP_ACC.1)

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

Security attribute based access control (FDP_ACF.1)

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

- [authorized users: user identity and/or group membership associated with the user[4],
- DBMS-controlled objects: object identity, access control rules for the object, ownership of object and parent object].

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

- The Discretionary Access Control policy mechanism shall, either by explicit authorized user action or by default, provide that database management system controlled objects are protected from unauthorized access according to the following ordered rules:
  a) If the requested mode of access is denied to that authorized user deny access
  b) If the requested mode of access is denied to any group of which the authorized user is a member, deny access
  c) If the requested mode of access is permitted to that authorized user, permit access.
  d) If the requested mode of access is permitted to any group of which the authorized user is a member, grant access
  e) Else deny access].

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

- Authorized administrators, the owner of an object and owners of parent

[4] The Discretionary Access Control policy is not enforced on system internal tasks that are not associated with an identified user.

objects have access
- in case of Ownership-Chaining access is always granted].

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

Subset residual information protection (FDP_RIP.1)

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 [objects that are related to or may be exposed through user sessions].

6.1.3 Class FIA: Identification and authentication

User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 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
- [login-type (SQL-Server login or Windows Account Name)]].

Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [no TSF mediated actions] on behalf of the user to be performed before the user is authenticated.

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

Application Note: The TSF shall provide
- SQL Server Authentication and
- Access to Windows Authentication

to support user authentication.

The TSF shall authenticate any user's claimed identity according to the following rules:
- If the login is associated with a Windows user or a Windows group Windows Authentication is used,
- If the login is a SQL Server login the SQL Server authentication is used.

Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow [no TSF-mediated actions] on behalf of the user to be performed before the user is identified.

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

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

FIA_USB_(EXT).2.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [the list of the security attributes as defined in FIA_ATD.1.1].
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: [none].
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: [none].
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: [none].

6.1.4 Class FMT: Security Management

Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1.1	The TSF shall restrict the ability to *disable and enable* the functions [relating to the specification of events to be audited] to [authorized administrators].

Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1	The TSF shall enforce the [Discretionary Access Control policy] to restrict the ability to *manage* [all] the security attributes to [authorized administrators].
Application Note:	This restriction includes the management of the security attributes defined in FIA_ATD.1.

Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1	The TSF shall enforce the [Discretionary Access Control policy] to provide *restrictive* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow ~~**the**~~ [no user] to specify alternative initial values to override the default values when an object or information is created.

Management of TSF data (FMT_MTD.1)

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

Revocation (FMT_REV.1(1))

FMT_REV.1.1(1)	The TSF shall restrict the ability to revoke [the list of the security attributes as defined in FIA_ATD.1.1] associated with the *users* under the control of the TSF to [the authorized administrator].
FMT_REV.1.2(1)	The TSF shall enforce the rules [Changes to logins are applied at the latest as soon as a new session for the login is established].

Revocation (FMT_REV.1(2))

FMT_REV.1.1(2) The TSF shall restrict the ability to revoke [the list of security attributes as defined in FDP_ACF.1.1] 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**.

FMT_REV.1.2(2) The TSF shall enforce the rules [The changes have to be applied immediately].

Specification of Management Functions (FMT_SMF.1)

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

- Add and delete logins
- Add and delete users
- Change role membership for DB scoped roles and Server scoped roles
- Create and destroy database scoped groups
- Create, Start and Stop Audit
- Include and Exclude Auditable events
- Define the mode of authentication
- Manage Attributes for Session Establishment
- Define the action to take in case the audit file is full]

Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [authorized administrator and [roles as defined in the following tables; roles to be defined by authorized administrators]].

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

Table 12 – Default Server Roles

Role	Description
sysadmin	Members of the sysadmin fixed server role can perform any activity in the server. By default, all members of the Windows BUILTIN\Administrators group, the local administrator's group, are members of the sysadmin fixed server role.
serveradmin	Members of the serveradmin fixed server role can change server-wide configuration options and shut down the server.
securityadmin	Members of the securityadmin fixed server role manage logins and their properties. They can GRANT, DENY, and REVOKE server-level permissions. They can also GRANT, DENY, and REVOKE database-level permissions. Additionally, they can reset passwords for SQL Server logins.
processadmin	Members of the processadmin fixed server role can end processes that are running in an instance of SQL Server.
setupadmin	Members of the setupadmin fixed server role can add and remove linked servers.
bulkadmin	Members of the bulkadmin fixed server role can run the BULK INSERT

	statement.
diskadmin	The diskadmin fixed server role is used for managing disk files.
dbcreator	Members of the dbcreator fixed server role can create, restore and drop any database, and can alter their own databases.

Table 13 – Default Database Roles

Role	Granted Permission(s)
db_owner	Members of the db_owner fixed database role can perform all configuration and maintenance activities on the database, and can also drop the database.
db_securityadmin	Members of the db_securityadmin fixed database role can modify role membership and manage permissions. Adding principals to this role could enable unintended privilege escalation.
db_accessadmin	Members of the db_accessadmin fixed database role can add or remove access to the database for Windows logins, Windows groups, and SQL Server logins.
db_backupoperator	Members of the db_backupoperator fixed database role can back up the database.
db_ddladmin	Members of the db_ddladmin fixed database role can run any Data Definition Language (DDL) command in a database.
db_datawriter	Members of the db_datawriter fixed database role can add, delete, or change data in all user tables.
db_datareader	Members of the db_datareader fixed database role can read all data from all user tables.
db_denydatawriter	Members of the db_denydatawriter fixed database role cannot add, modify, or delete any data in the user tables within a database.
db_denydatareader	Members of the db_denydatareader fixed database role cannot read any data in the user tables within a database.

6.1.5 Class FPT: Protection of the TOE Security Functions

Internal TSF consistency (FPT_TRC.1)

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

FPT_TRC.1.2 When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [no function, since the TOE does not contain physically separated parts].

6.1.6 Class FTA: TOE Access

Basic limitation on multiple concurrent sessions (FTA_MCS.1)

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 [*5*] sessions per user.

TOE access information (FTA_TAH_(EXT).1)

FTA_TAH_(EXT).1.1 Upon a session establishment, the TSF shall store

a. the [date and time] of the session establishment attempt of the user.
b. the incremental count of successive unsuccessful session establishment attempt(s).

FTA_TAH_(EXT).1.2 Upon successful session establishment, the TSF shall allow the [date and time] of

a. the previous last successful session establishment, and
b. the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the previous last successful session establishment

to be retrieved by the user.

TOE session establishment (FTA_TSE.1)

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [attributes that can be set explicitly by authorized administrator(s), including user identity, and *time of day, day of the week*]

6.2 TOE Security Assurance Requirements

The assurance requirements for the TOE comprise all assurance requirements for EAL 4 as defined in [CC] augmented by ALC_FLR.2.

6.3 Security Requirements rationale

6.3.1 Security Functional Requirements rationale

The following table contains the rationale for the TOE Security Requirements. This rationale has been directly taken from [PP] with the exception of O.ACCESS_HISTORY which has been taken from [EP].

Table 14 - Rationale for TOE Security Requirements

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS_HISTORY The TOE will store information related to previous attempts to establish a session and make that information available to the user.	FTA_TAH_(EXT).1	The TOE must be able to store and retrieve information about previous unauthorized login attempts and the number of times the login was attempted every time the user logs into their account. The TOE must also store the last successful authorized login. This information will include the date, time, method, and location of the attempts. When appropriately displayed, this will allow the user to

Objective	Requirements Addressing the Objective	Rationale
		detect if another user is attempting to access their account. These records should not be deleted until after the user has been notified of their access history. (FTA_TAH_(EXT).1)
O.ADMIN_ROLE The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.	FMT_SMR.1	The TOE will establish, at least, an authorized administrator role. The ST writer may choose to specify more roles. The authorized administrator will be given privileges to perform certain tasks that other users will not be able to perform. These privileges include, but are not limited to, access to audit information and security functions. (FMT_SMR.1)
O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security relevant events associated with users.	FAU_GEN.1 FAU_GEN.2 FAU_SEL.1	FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that the administrator has the ability to audit any security relevant events that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements a ST author adds to this PP.[5] FAU_GEN.2 ensures that the audit records associate a user and any associated group identity with the auditable event. In the case of authorized users, the association is accomplished with the user ID. In the case of authorized groups, the association is accomplished with the group ID. FAU_SEL.1 allows the administrator to configure which auditable events will be recorded in the audit trail. This provides the administrator with the flexibility in recording only those events that are deemed necessary by site policy, thus reducing the amount of resources consumed by the audit

[5] No additional security functional requirements were added by the ST author.

Objective	Requirements Addressing the Objective	Rationale
		mechanism.
O.DISCRETIONARY_ ACCESS The TSF must control access of subjects and/or users to named resources based on identity of the object, subject or user. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.	FDP_ACC.1 FDP_ACF.1	The TSF must control access to resources based on the identity of users that are allowed to specify which resources they want to access for storing their data. The access control policy must have a defined scope of control [FDP_ACC.1]. The rules for the access control policy are defined [FDP_ACF.1].
O.I&A The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.	FIA_ATD.1 FIA_UAU.1 FIA_UID.1 FIA_USB_(EXT).2	The TSF must ensure that only authorized users gain access to the TOE and its resources. Users authorized to access the TOE must use an identification and authentication process [FIA_UID.1, FIA_UAU.1]. To ensure that the security attributes used to determine access are defined and available to the support authentication decisions. [FIA_ATD.1]. Proper authorization for subjects acting on behalf of users is also ensured [FIA_USB_(EXT).2]. The appropriate strength of the authentication mechanism is ensured.
O.MANAGE The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_REV.1(1) FMT_REV.1(2) FMT_SMF.1	FMT_MOF.1 requires that the ability to use particular TOE capabilities be restricted to the administrator. FMT_MSA.1 requires that the ability to perform operations on security attributes be restricted to particular roles. FMT_MSA.3 requires that default values used for security attributes are restrictive.

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

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

6.3.2 Rationale for satisfying all Dependencies

The following table contains the rationale for satisfying all dependencies of the Security Requirements. This rationale has been taken from [PP] with the addition of the entry of FTA_TAH_(EXT)1 from [EP].

Table 15 - Rationale for satisfying all dependencies

Requirement	Dependency	Satisfied
FAU_GEN.1	FPT_STM.1	This requirement is satisfied by the assumption on the IT environment, given in A.SUPPORT.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	satisfied by FAU_GEN.1 satisfied by FIA_UID.1
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	satisfied by FAU_GEN.1 satisfied by FMT_MTD.1
FDP_ACC.1	FDP_ACF.1	satisfied by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1	satisfied by FDP_ACC.1

Requirement	Dependency	Satisfied
	FMT_MSA.3	satisfied by FMT_MSA.3.
FDP_RIP.1	None	N/A
FIA_ATD.1	None	N/A
FIA_UAU.1	FIA_UID.1	satisfied by FIA_UID.1
FIA_UID.1	None	N/A
FIA_USB_(EXT).2	FIA_ATD.1	satisfied by FIA_ATD.1
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	satisfied by FMT_SMF.1 satisfied by FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	satisfied by FDP_ACC.1. satisfied by FMT_SMF.1 satisfied by FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	satisfied by FMT_MSA.1 satisfied by FMT_SMR.1
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	satisfied by FMT_SMF.1 satisfied by FMT_SMR.1
FMT_REV.1(1)	FMT_SMR.1	satisfied by FMT_SMR.1
FMT_REV.1(2)	FMT_SMR.1	satisfied by FMT_SMR.1
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	satisfied by FIA_UID.1
FPT_TRC.1	FPT_ITT.1	FPT_ITT.1 is not applicable For a distributed TOE the dependency is satisfied through the assumption on the environment, A.CONNECT , that assures the confidentiality and integrity of the transmitted data[6]
FTA_MCS.1	FIA_UID.1	satisfied by FIA_UID.1

[6] The TOE does not contain physically separated parts.

Requirement	Dependency	Satisfied
FTA_TAH_(EXT).1	None	N/A
FTA_TSE.1	None	N/A

6.3.3 Rationale for extended requirements

Table 16 presents the rationale for the inclusion of the extended functional requirements as already given in [PP] and [EP] respectively.

Table 16 - Rationale for Explicit Requirements

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

6.3.4 Rationale for Assurance Requirements

To be resistant against attacks that are performed by attackers with an attack potential of enhanced basic and to gain a higher level of assurance in the correct implementation, EAL4 has been chosen. The additional use of ALC_FLR.2 is necessary in order to stay compliant to [PP].

7 TOE Summary Specification

This chapter presents an overview of the security functionality implemented by the TOE. Please note that the TOE does not contain physically separated parts, hence, the SFR FPT_TRC.1 is trivially met as intended by the application note in [PP, 7.1.5.1].

7.1 Security Management (SF.SM)

This security functionality of the TOE allows modifying the TSF data of the TOE and therewith managing the behavior of the TSF.

This comprises the following management functions (FMT_SMF.1):

- Add and delete logins on an instance level,
- Add and delete users on a database level,
- Change role membership for DB scoped roles and Server scoped roles,
- Create and destroy database roles,
- Create, Start and Stop Security Audit,
- Include and exclude Auditable events,
- Define the mode of authentication for every login,
- Manage attributes for Session Establishment,
- Define the action to take in case the audit file is full.

All these management functions are available via T-SQL statements directly or realized by Stored Procedures within the TOE which can be called using T-SQL.

The TOE maintains a set of roles on the server level and on the database level as listed in Table 12 and Table 13. The TOE maintains a security ID for each login on a server level and each database user. This security ID is used to associate each user with his assigned roles (FIA_ATD.1, FIA_USB_(EXT).2, FMT_SMR.1).

Changes to logins that are preformed via the management functions are applied at the latest as soon as a new session for the login is established (FMT_REV.1(1)).

7.2 Access Control (SF.AC)

The TOE provides a Discretionary Access Control (DAC) mechanism to control the access of users to objects based on the identity of the user requesting access, the membership of this user to roles, the requested operation and the ID of the requested object.

The TOE maintains two kinds of user representations:

1. On an instance level an end user is represented by a login. On this level the TOE controls the access of logins to objects pertaining to the instance (e.g. to view a database).
2. On a database level an end user is represented by a database user. On this level the TOE controls the access of database users to objects of the database (e.g. to read or create a table).

Further the TOE is able to manage a user account completely within a database. In this case the user account in the database is associated with a login that is also contained in this database. The authentication then happens against this database.

Members of the database roles “db_owner” or “db_accessadmin” are able to add users to a database. The TOE maintains an internal security identifier (SID) for every user and role. Each database user can be associated with at most one instance “login”.

Every object controlled by the TOE has an ID, an owner and a name.

Objects in the TOE form a hierarchy and belong to one of three different levels: server, database and schema.

The TOE maintains an Access Control List (ACL) for each object within its scope. These ACLs are stored in a system table which exists in every database for database related ACLs and in a system table in the ‘master’ database for instance level ACLs.

Each entry of an ACL contains a user SID and defines whether a permission is an “Allow” or a “Deny” permission for that SID.

When a new object is created, the creating user is assigned as the owner of the object and has complete control over the object. The initial ACL for a newly created object is always empty by default and cannot be overridden by any role (FMT_MSA.3).

After creation, grant, deny or revoke permissions on objects can be assigned to users. Changes to the security relevant attributes of objects are immediately applied (FMT_REV.1(2)).

When a user attempts to perform an action to an object under the control of the TOE, the TOE decides whether the action is to be permitted based on the following rules:

1. If the requested mode of access is denied to that authorized user, the TOE will deny access
2. If the requested mode of access is denied to any role of which the authorized user is a member, the TOE will deny access
3. If the requested mode of access is permitted to that authorized user, the TOE will permit access
4. If the requested mode of access is permitted to any role of which the authorized user is a member, the TOE will permit access
5. Else: The TOE will deny access

The TOE permission check for an action on an object includes the permissions of its parent objects. The permissions for the object itself and all its parent objects are accumulated together before the aforementioned rules are evaluated. Note: Some actions require more than one permission.

This means that if a user or a role has been granted a permission to an object this permission is also valid for all child objects. E.g. if a user has been granted a permission to a schema, he automatically has the same permission on all tables within that schema, if the permission has not explicitly been denied. Similarly, if a user has been denied a permission on a schema, he will be denied the same permission to all tables within that schema, regardless of explicit grant permissions.

The rules as described before are always applied when a user requests access to a certain object using a certain operation. There are only two situations where these access control rules are overridden:

1. The system administrator, the owner of an object and owners of parent objects always have access, so for these users the TOE will always allow access to the object
2. In the case of “Ownership Chaining” which is described in chapter 8.1 in more detail the access is allowed

(FDP_ACC.1 and FDP_ACF.1)

As the access to management functions of the TOE is controlled by the same functionality as the access to user data this security functionality additionally ensures that the management functions are

only available for authorized administrators (FMT_MOF.1, FMT_MSA.1, FMT_MTD.1, FMT_REV.1(1)).

7.3 Identification and Authentication (SF.I&A)

This security functionality requires each user to be successfully authenticated before allowing any other actions on behalf of that user. This is done on an instance level and means that the user has to be associated with a login of the TOE.

The TOE knows two types of logins: Windows accounts and SQL Server logins. The administrator has to specify the type of login for every login he is creating.

The possibility for the TOE to perform its own authentication is necessary because not all users connecting to the TOE are connecting from a Windows environment.

Microsoft Windows account names

These logins are associated with a user account of the Windows Operating System in the environment.

For these logins the TOE requires that the Windows environment passes on the Windows SID(s) of that user to authenticate the user before any other action on behalf of that user is allowed.[7]

For these logins the Windows security identifier (SID) from the Windows account or group is used for identification of that login within the TOE. Any permission is associated with that SID (FIA_UAU.1, FIA_UID.1, FIA_ATD.1, FIA_USB_(EXT).2).

SQL Server login names

SQL Server logins are not associated with a user of Windows but are maintained by the TOE itself. Logins exist on a server level (and users in databases can be associated with a login) and on a database level itself (for contained databases). For every SQL Server login the TOE maintains a login name and a password. The password is not stored in plain text, but hashed using the SHA2-512 hash function provided by the Operating System in the environment.

Each SQL Server login name is stored in a system table. SQL Server generates a SID that is used as a security identifier and stores it in this table.

This SID is internally used as a security identifier for the login.
If a user is connecting to the TOE using a SQL Server login he has to provide the username and password. The TOE hashes the password using the hash function provided by the Operating System in the environment, and compares the hash to the value stored for that user. If the values are identical the TOE has successfully authenticated the user (FIA_UAU.1, FIA_UID.1, FIA_ATD.1, FIA_USB_(EXT).2).

If the binding of a user security attribute to a subject fails at login (e.g., role membership), the login will also fail, and the failure of the login will be audited (FIA_USB_(EXT).2, FAU_GEN.1).

[7] Windows authentication of users may be based on a username and password or alternative mechanisms. After successful authentication of a user Windows associates a list of SID(s) with every user which represent the user and every group the user is a member of.

7.4 Security Audit (SF.AU)

The TOE produces audit logs for all security relevant actions. These audit logs are stored into files in the environment of the TOE.

The Security Audit of the TOE especially comprises the following events:

- Startup and Shutdown of the TOE,
- Start and Shutdown of Security Audit Function,
- Every login attempt including the processes for authentication and session establishment,
- Every successful request to perform on operation on an object covered by the access control function,
- Modifications to the role membership of users,
- The use of SF.SM,
- Every rejected attempt to establish a session.

The TOE maintains a set of events which can be additionally audited and provides the administrator with the capability to start a Security Audit process to capture these events.

For each event in the Security Audit logs the following information is stored:

1. Date and Time of the event,
2. Identity of the user causing the event (if available),
3. Type of the event,
4. ID of the object,
5. Outcome (success or failure) of the event.

Furthermore each audit file contains an introduction with the list of events which are audited in the file (FAU_GEN.1 and FAU_GEN.2).

The administrator has the possibility to specify, what should happen in case an audit file is full. The following two scenarios are supported in the evaluated version:

1. Rollover

   The administrator specifies a maximum size per audit file and a maximum number of files for the Security Audit. If one audit file is full, the TOE starts the next file until the maximum number of files has been reached. When the maximum number of files has been reached and the last audit file is full, the TOE will start overwriting the oldest audit file.

2. Shutdown

   The administrator specifies one audit file with a maximum size and the option to shut down the TOE on any audit error. When the maximum size of the audit file has been reached the TOE will stop operation.

The TOE provides the possibility to create a filter for the audit function. Using this filter mechanism the administrator is able to exclude auditable events from being audited based on the following attributes:

- User identity,
- Event Type,
- Object identity,
- Success or failure of auditable security events.

However, to modify the behavior of the Security Audit function by including additional or excluding events from being audited the administrator has to stop the Security Audit process, modify the Security Audit function and start the Security Audit process again. The event types to be audited are defined by

Audit Action Groups which allow including or excluding classes of audit events on a server-level, database-level and audit-level (FAU_SEL.1).

7.5 Session Handling (SF.SE)

After a user attempting to establish a session has been successfully authenticated by SF.I&A this security functionality decides whether this user is actually allowed to establish a session to the TOE.

The TOE uses two sets of additional criteria to decide whether a user is allowed to establish a session. First the TOE enforces a limit of the number of concurrent sessions a user is allowed to have at one time. This limit is set to 5 by default but can be modified by authorized administrators as described in SF.SM. If a user reached the limit of concurrent sessions the TOE will deny establishing another session for that user (FTA_MCS.1).

As a second criterion the admin is able to specify a set of rules to explicitly deny session establishment based on:

- User's identity,
- Time of the day, and
- Day of the week.

The TOE only establishes a session for a user if no explicit deny rule for that user has been specified (FTA_TSE.1).

For every attempt to establish a session (whether successful or not) the TOE stores the date and time of the event and the number of unsuccessful attempts since the last successful attempt. This information is available at the client interface at any time. It is not erased but only overwritten with updated values between sessions, i.e. the time of the last successful logon, the time of the last unsuccessful logon and the number of unsuccessful logon attempts between the last successful logon and the current successful logon are available until the user logs out (FTA_TAH._(EXT).1).

After the TOE established a session to a user the user context is held in a context with limited permission. SF.SE maintains a separate context for the execution of each operation by a user. As soon as a user performs an operation on an object the TOE starts at least one thread to perform this operation.

When the TOE reuses memory which could contain previous information content and which is related to the context of a user's session (i.e. to which a user could gain access), this previous information will not be available for any user. To ensure this, the TOE either directly overwrites any memory that will be used for users sessions completely with new information or with a certain pattern. Before the previous information has been overwritten the resource is not available for any usage. For memory which is allocated using the Operating System the TOE uses a function of the OS, which ensures that only empty memory is provided to the TOE. Whenever data is written to or loaded from disc this is done page wise where a page has the size of 8 KB (FDP_RIP.1).

8 Appendix

8.1 Concept of Ownership Chains

Database Objects within the TOE are not always only passive objects. Some objects refer to other objects. This is especially true for Stored Procedures and Views. When multiple database objects access each other sequentially, the sequence is known as a chain. Although such chains do not independently exist, when the TOE traverses the links in a chain, the TOE evaluates access permissions on the constituent objects differently than it would if it were accessing the objects separately. These differences have important implications for managing security.

Ownership chaining enables managing access to multiple objects, such as multiple tables, by setting permissions on one object, such as a view. Ownership chaining also offers a slight performance advantage in scenarios that allow for skipping permission checks.

8.1.1 How Permissions Are Checked in a Chain

When an object is accessed through a chain, the TOE first compares the owner of the object to the owner of the calling object. This is the previous link in the chain. If both objects have the same owner, permissions on the referenced object are not evaluated. In the context of the Discretionary Access Control Mechanism this is not a circumvention of access control as the owner of an object always has complete control over his objects. So if one user is the owner of both objects, the calling object and the called object, the owner also would have direct access to both objects.

8.1.2 Example of Ownership Chaining

In the following illustration, the July2003 view is owned by Mary. She has granted to Alex permissions on the view. He has no other permissions on database objects in this instance. What happens when Alex selects the view?

Alex executes SELECT * on the July2003 view. The TOE checks permissions on the view and confirms that Alex has permission to select on it.

The July 2003 view requires information from the SalesXZ view. The TOE checks the ownership of the SalesXZ view. Because this view has the same owner (Mary) as the view that calls it, permissions on SalesXZ are not checked. The required information is returned.

The SalesXZ view requires information from the InvoicesXZ view. The TOE checks the ownership of the InvoicesXZ view. Because this view has the same owner as the previous object, permissions on InvoicesXZ are not checked. The required information is returned. To this point, all items in the sequence have had one owner (Mary). This is known as an unbroken ownership chain.

The InvoicesXZ view requires information from the AcctAgeXZ view. The TOE checks the ownership of the AcctAgeXZ view. Because the owner of this view is different from the owner of the previous object (Sam, not Mary), full information about permissions on this view is retrieved. If the AcctAgeXZ view has permissions that allow access by Alex, information will be returned.

The AcctAgeXZ view requires information from the ExpenseXZ table. The TOE checks the ownership of the ExpenseXZ table. Because the owner of this table is different from the owner of the previous object (Joe, not Sam), full information about permissions on this table is retrieved. If the ExpenseXZ table has permissions that allow access by Alex, information is returned.

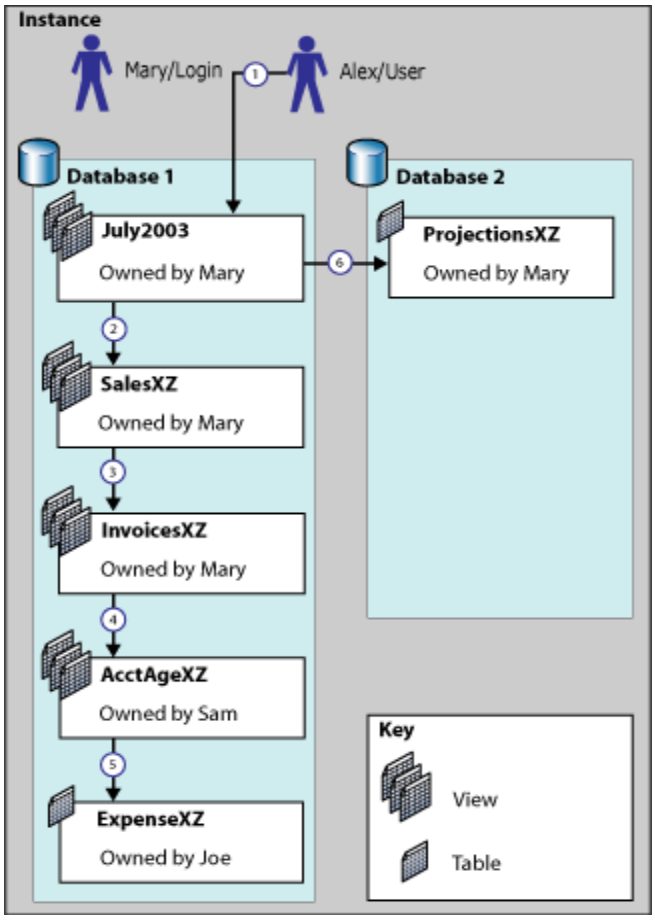

Figure 2 - Concept of Ownership Chaining

When the July2003 view tries to retrieve information from the ProjectionsXZ table, the TOE first checks to see whether cross-database chaining is enabled between Database 1 and Database 2. If cross-database chaining is enabled, the TOE will check the ownership of the ProjectionsXZ table. Because this table has the same owner as the calling view (Mary), permissions on this table are not checked. The requested information is returned.

8.2 References

The following documentation was used to prepare this ST:

[AGD] SQL Server 2017 Technical Documentation

[AGD_ADD] SQL Server 2017 Database Engine Common Criteria Evaluation – Guidance Addendum (delivered via https://www.microsoft.com/en-us/sql-server/data-security (click on “View our Common Criteria certification”))

[CC] Common Criteria for Information Technology Security Evaluation

Part 1: Introduction and general model, dated April 2017, version 3.1 R5

Part 2: Security functional requirements, dated April 2017, version 3.1, R5

Part 3: Security assurance requirements, dated April 2017, version 3.1, R5

[PP] DBMS Working Group Technical Community Protection Profile for Database Management Systems (DBMS PP) Base Package, Version 2.12, March 23rd, 2017 ([PP])

[EP] DBMS Working Group Technical Community DBMS Protection Profile Extended Package - Access History (DBMS PP_EP_AH), Version 1.02, March 23rd, 2017 ([EP])

8.3 Glossary and Abbreviations

8.3.1 Glossary

The following terms are used in this Security Target:

Term	Definition
Attacker	The term attacker refers to any individual (or technical entity) that is attempting to subvert the security functionality of the TOE. In this Security Target it is assumed that the attacker has an attack potential of “enhanced basic”.
Authorized Administrators	This term refers to a group of users which comprise the “sysadmin” (sa) and any user who is allowed to perform a management operation because the permission has been granted to him within the DAC either by assigning him to a role with administrator permissions or by granting him the possibility to perform an administrative operation explicitly.
DAC	Discretionary Access Control is a mechanism to limit the access of users to objects based on the ID of the user, the ID of the object and a set of access control rules.
DBMS	A DBMS is a computerized repository that stores information and allows authorized users to retrieve and update that information.
Named Pipe	Method for inter process communication.
Object	An object within the TOE contains data and can be accessed by subjects. However in the TOE an object is not necessarily only a passive entity as some objects refer to other objects.
OC	Ownership Chaining.
SQL	The Structured Query Language is a language which can be used to create, modify and retrieve data from a DBMS.
SQL Server	SQL Server is a product of Microsoft to which the TOE belongs.
TDS	Tabular Data Stream is a data format which is used for communication with the TOE.
T-SQL	Extension of the SQL language in order to support control flow, variables, user authentication and various other functions.
User	The term user refers to technical entities (e.g. applications, other instances of the TOE) or human users (using a SQL-client) that are using the services of the TOE.

8.3.2 Abbreviations

The following abbreviations are used in this Security Target:

Abbreviation	Definition
ACL	Access Control List
CC	Common Criteria
DAC	Discretionary Access Control

Abbreviation	Definition
DBMS	Database Management System
EAL	Evaluation Assurance Level
ETL	Extract, Transform, Load
IT	Information Technology
MOM	Microsoft Operations Manager
MS	Microsoft
NIAP	National Information Assurance Partnership
NSA	National Security Agency
OLAP	Online analytical processing
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Functionality
SFR	Security Functional Requirement
SID	Security ID
SMS	System Management Server
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functionality
T-SQL	Transact SQL