Siebel

Siebel eBusiness Platform™ V7.8.2

Security Target V2.0

Debra Baker

November 9, 2005

Suite 100 West♦7925 Jones Branch Drive♦McLean, VA 22102-3305♦703 848-0883♦Fax 703 848-0960

Revision History:

Date:	Version:	Author:	Description
1/30/2004	1.0	Debra Baker	Draft
11/09/05	2.0	Debra Baker	Final

TABLE OF CONTENTS

SECTION **PAGE**

Table of Tables and Figures

1 Security Target Introduction

1.1 Security Target Identification

TOE Identification: Siebel eBusiness Platform V7.8.2
ST Title: Siebel eBusiness Platform V7.8.2 Security Target
ST Version: Version 2.0
ST Authors: Debra Baker
ST Date: November 9, 2005
Assurance Level: EAL2
Strength of Function: SOF Basic
Registration: <To be filled in upon registration>
Keywords: Access Control, Security Target, and Security Management

1.2 Security Target Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for Siebel *e*Business Platform Version 7.8.2. Siebel *e*Business Platform is an application platform upon which all Siebel *e*Business Applications are developed and deployed. Based on the Siebel Smart Web Architecture, the Siebel *e*Business Platform provides a complete suite of configuration and operational tools and services including:

- graphical user interface,
- data synchronization and replication,
- workflow,
- data categorization into various catalogs and categories of data,
- user assignments to administrative responsibilities,
- user assignments to groups based on division, position, organization, and access groups,
- security.

These tools and services are leveraged across all Siebel *e*Business Applications. The following security functionality is provided: User data protection (access control), security audit, security management.

1.3 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 from the Common Criteria Version 2.2 Rev 256 CCIMB-2004-01-001 January 2004.

1.4 Document Organization

The main sections of an ST are the ST Introduction, Target of Evaluation (TOE) Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, and Rationale.

Section 2, the TOE Description, describes the product type and the scope and boundaries of the TOE.

Section 3, TOE Security Environment, identifies assumptions about the TOE's intended usage and environment and threats relevant to secure TOE operation.

Section 4, Security Objectives, defines the security objectives for the TOE and its environment.

Section 5, IT Security Requirements, specifies the TOE Security Functional Requirements (SFR), Security Requirements for the IT Environment, and the Security Assurance Requirements.

Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures.

Section 7, Protection Profile (PP) Claims, is not applicable, as this product does not claim conformance to any PP.

Section 8, Rationale, presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

Section 9 and 10, provide acronym definitions and references.

1.5 Terminology

Table 1-1 Terminology

Term	Definition
access control mechanisms	Access control mechanisms that are applied to parties and data determines what data a user sees.
customer data	This data includes contacts and transactional data such as opportunities, orders, quotes, service requests, and accounts. For Customer data, access is controlled at the data item level.
master data	This data includes the following referential data: products, literature, solutions, resolution items, decision issues, auctions, events, training courses, and competitors. Master data can be organized into catalogs, which are hierarchies of categories. By categorizing master data, access can be controlled at the catalog and category levels through access groups.
organization	A branch of an agency or a division of a company – is a hierarchy of positions. Those employees assigned to a position within a certain organization are granted access to the data that has been assigned to that organization.
other data	This data includes referential data that is not master data, such as price lists, cost lists, rate lists, and Smartscripts.
position	A position is a job title in a division of an internal or partner organization. In the TOE, this is a security attribute that access control is based on.
Responsibilities	User responsibilities are defined as 'roles' in Siebel eBusiness Platform terminology; therefore, for consistency we have used the word responsibility instead of role. 'Responsibilities' is also used as a label for the security attribute as defined in FDP_ACF.
Roles	Siebel terminology for roles is the security attribute called Responsibilities. All provided guidance manuals for CC evaluation refer to 'responsibilities'. Common Criteria uses 'roles' to identify specific user groupings (account types) such as administrator or operator. The ST author has attempted to only use the term 'role' only when referring to CC Part 2 wording such as in FMT_SMR.1
Administrator	There are two types of administrator roles defined in the ST: Siebel Administrator and Custom Administrator. When the ST text uses the term "administrator" without specifying a particular type of administrator, it is implied that the text is referring to all types of administrators, i.e. the Siebel Administrator and Custom Administrators.

2 TOE Description

2.1 Product Type

Siebel eBusiness Platform is an application platform which provides a complete suite of configuration and operational tools and services including interfaces, data synchronization and replication, workflow, assignment, and security. An application platform masks the underlying specificity of the development environment, specifically the Operating System (OS) and the Database Management System (DBMS). This enables the development of applications that are independent of the hardware and OS platforms and of the programming language. All Siebel eBusiness Applications are developed and deployed atop the Siebel eBusiness Platform. Siebel *e*Business Platform is based on an object architecture in which the user interface, logic, and data are separated into four clearly delineated logical layers: physical User Interface (UI) rendering, logical UI definition, business logic, and data access. This object architecture provides enhancements without having to replace the existing underlying architecture.

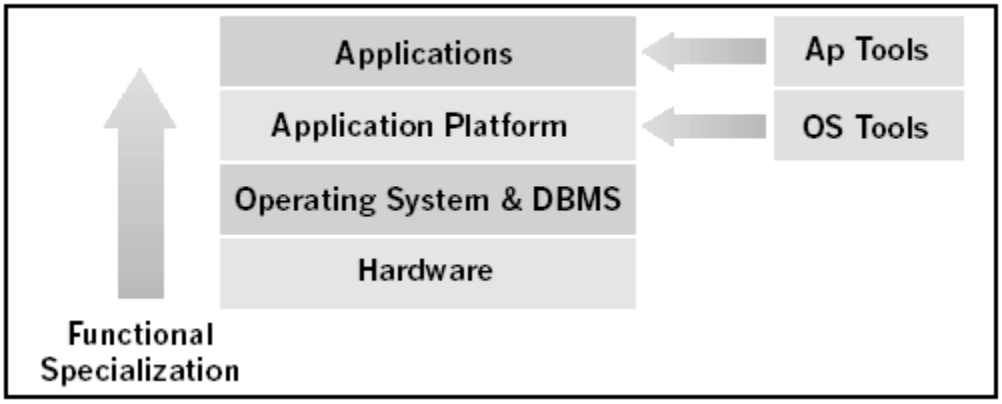

Figure 2-1 Application Platform Architecture

An application platform is a set of services and tools built on top of an OS and DBMS to support a specific application domain. The platform greatly facilitates the construction of new applications, as it provides all the basic mechanisms that are at the very nature of these applications.

2.2 Siebel eBusiness Platform Components

The Siebel *e*Business Platform consists of the Siebel Application Server, Database Server, LDAP Directory Server used for authentication, and Graphical User Interface. The TOE Components are the Siebel Application Server and Graphical User Interface. The TOE components provide all of the configuration and operational tools and services described in section 2.1. The Database Server and the LDAP server are not within the TOE boundary, but instead are part the environment in which the TOE operates (See Figure 2-3).

2.2.1 Siebel eBusiness Graphical User Interface

Siebel eBusiness platform has a graphical user interface through which all Siebel eBusiness security functions are managed and user operations are performed. This same interface is used by all account holders for both administration purposes and for end-user product usage. In any case, users interact with the Siebel Application Server via a standard web browser, such as Internet Explorer (version 5.5 or greater) or Netscape Communicator (version 7.0.2 or greater). The

Graphical User interface presents the user with a login screen and collects the identification and authentication data from the user. The Graphical User interface passes this user login information to the Siebel Application Server.

- **Administrator Interface**

The Administrator Interface is a GUI interface that serves as the primary administrative view of the product. Through this interface, administrators manage audit functions, user accounts, and assign the responsibilities in the Siebel system. Administrators use a web browser on their workstations to interact with the Siebel Application server. In addition, security policy settings for passwords are also established through this GUI.

- Security Audit: The administrator Interface serves as the mechanism for configuring the audit and searching, sorting, and viewing audit records.
- Security Management: The administrator Interface serves as the TOE external interface for administrators to manage the TOE security functions and data in the Siebel application server.

- **User Interface**

The Siebel User Interface presents a limited view of the Siebel system that is specifically tailored to users without administrative capabilities. Users can change their passwords associated with their accounts. Users are able to access folders and projects that they are assigned to.

2.2.2 Siebel Application Server

The Siebel Application Server (SAS) runs on a server host. The Siebel Application Server provides the core business logic of the application. The Siebel Application Server receives the user login information from the Graphical User Interface and sends it to the LDAP Server to check the validity of the username and password. As such, all other Siebel components communicate with the SAS. The application server performs the following security functions:

- User data protection (Access Control): Account holders have varying responsibilities. The TOE separates the account holders into various responsibilities by assigning the following account types: Siebel Administrator, customer defined administrator, and user. Each account holder is granted with various privilege levels for performing assigned responsibilities. The user privilege levels control access to data and functions that are protected by the TOE. The user account holders are restricted to data to which they have been explicitly granted access privileges.

  Siebel applications use two primary access control mechanisms:

  - **View level access control** - View level access control determines what parts of the Siebel application a user can access, based on the functions assigned to that user. In Siebel applications, these functions are called responsibilities. Responsibilities define the collection of views to which a user has access privileges. An employee assigned to one responsibility may not have access privileges to parts of the Siebel applications associated with another set of responsibilities.
  - **Record level access control** - Record level access control assigns access permissions to individual data items within an application. This allows administrators to authorize only those authenticated users that need to view particular data records to access that information. Siebel applications use four types of record level access control: division-based, position-based, organization-based, and access group-based. When a particular division position,

organization, or access group is assigned to a data record, only employees within that division, position, organization, or access group can view that record.

- Security Audit: The SAS generates an audit trail and stores it in the database. The SAS uses configuration data of an application to determine what events and information is to be audited. The CC configuration only includes one application which is the graphical user interface. When configured, SAS will audit the following events: creation, deletion, generated modifications, and copying of business component fields. These events include those caused by an administrator or end user. TSF data is viewed as stored information in fields within a business component. Siebel eBusiness Platform provides a utility for searching, sorting, and viewing audit records. CC users will need to ensure that the audit capability is turned on according to the supplied guidance.
- Security Management: The SAS performs the appropriate security management functions to manage the TOE security functions and data per administrator requests. The administrator requests are completed through the use of the Siebel eBusiness Graphical User Interface.
- Partial protection of TSF: The SAS protects its programs and data from unauthorized access through its own interfaces per the Siebel eBusiness Platform Access Control SFP (Table 5-2).

2.2.2.1 SAS Command Line Interface

Siebel Server Manager: The Siebel Server Manager (srvmgr) is an optional management and administration interface for the Siebel Server and Siebel Enterprise Server. The Siebel Server Manager allows you to configure the parameters governing the operation of each component, and determine which Siebel Servers a given component can operate. Use the Siebel Server Manager to:

- Start, Stop, Pause, and resume Siebel Servers, components, and tasks.
- Monitor the status and collect statistics across the Siebel Enterprise Server, Siebel Servers, components, and tasks.
- Manage the configuration of the Siebel Enterprise Server, Siebel Servers, components, and tasks.

All tasks that can be achieved using this CLI are included in the graphical user interface. The use and user of this command is audited and is kept in a separate audit log from the rest of the TOE.

The Siebel Server Manager command line interface will NOT be considered within the scope of this evaluation since all of the functions are covered within the GUI and it is preferable to have a single consolidated audit.

Therefore, for the purpose of this CC evaluation, the *srvmgr* CLI is considered part of the IT Environment and is outside the scope of the TOE. Product end users who want to maintain operations in compliance with the CC evaluation must not use this interface.

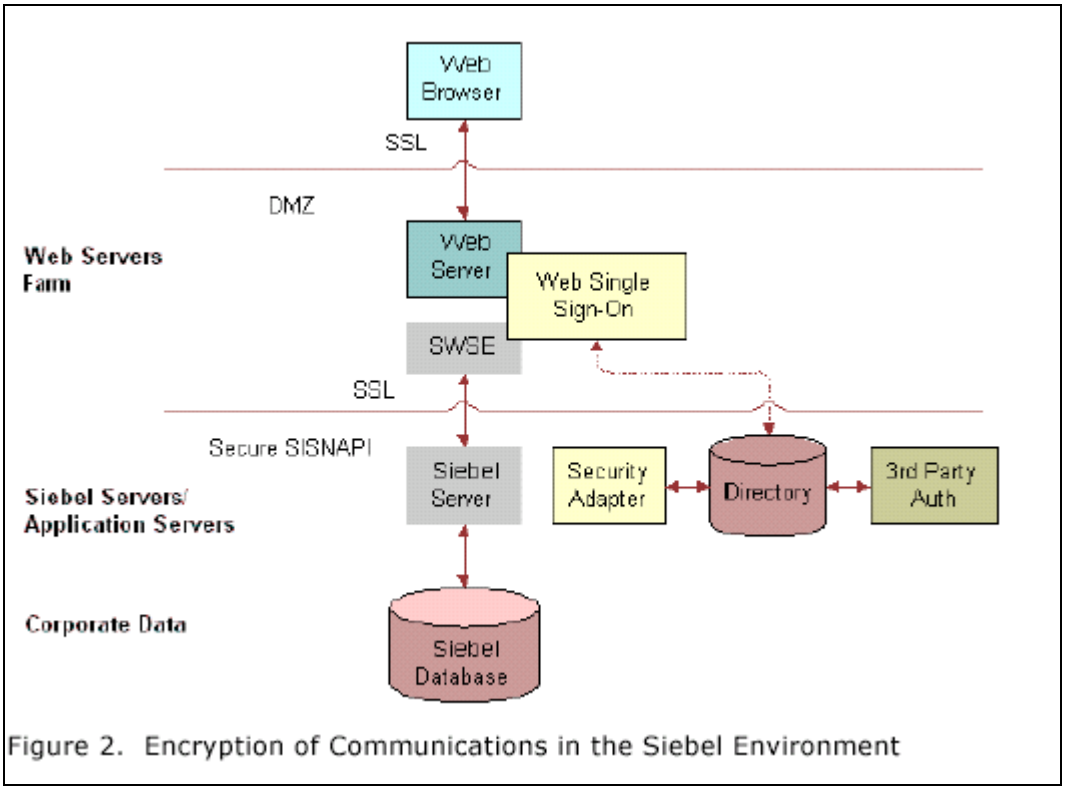

Figure 2. Encryption of Communications in the Siebel Environment

Figure 2-2 Siebel Architecture Diagram

2.3 TSF Physical Boundary and Scope of the Evaluation

The evaluated configuration includes the following:

- Siebel eBusiness Platform Application Server V7.8.2 (with the Strong Encryption Pack option) running on Microsoft Windows 2000 SP4 Server
- Siebel eBusiness Platform Application Server is accessible via the Administrator and Graphical User Interface using Internet Explorer V5.5 or greater running on Microsoft Windows 2000 SP4 workstation;

The TOE includes the Siebel Application Server and Siebel eBusiness Graphical User Interface (Administrator and User Interfaces).

The TOE does not include the following:

- The underlying operating system (OS) software and hardware,
- The third party relational database,
- The interface of the third party relational database,
- Third-party encryption software that is used to provide a trusted communication path between users and the TOE (Strong Encryption Pack provides the third party .dll files for stronger 128, 192, 256 bit encryption used in the CC testing),
- The LDAP Directory Server which is used for authentication purposes,
- The web browser that the Graphical User Interface relies on.
- the *srvmgr* CLI

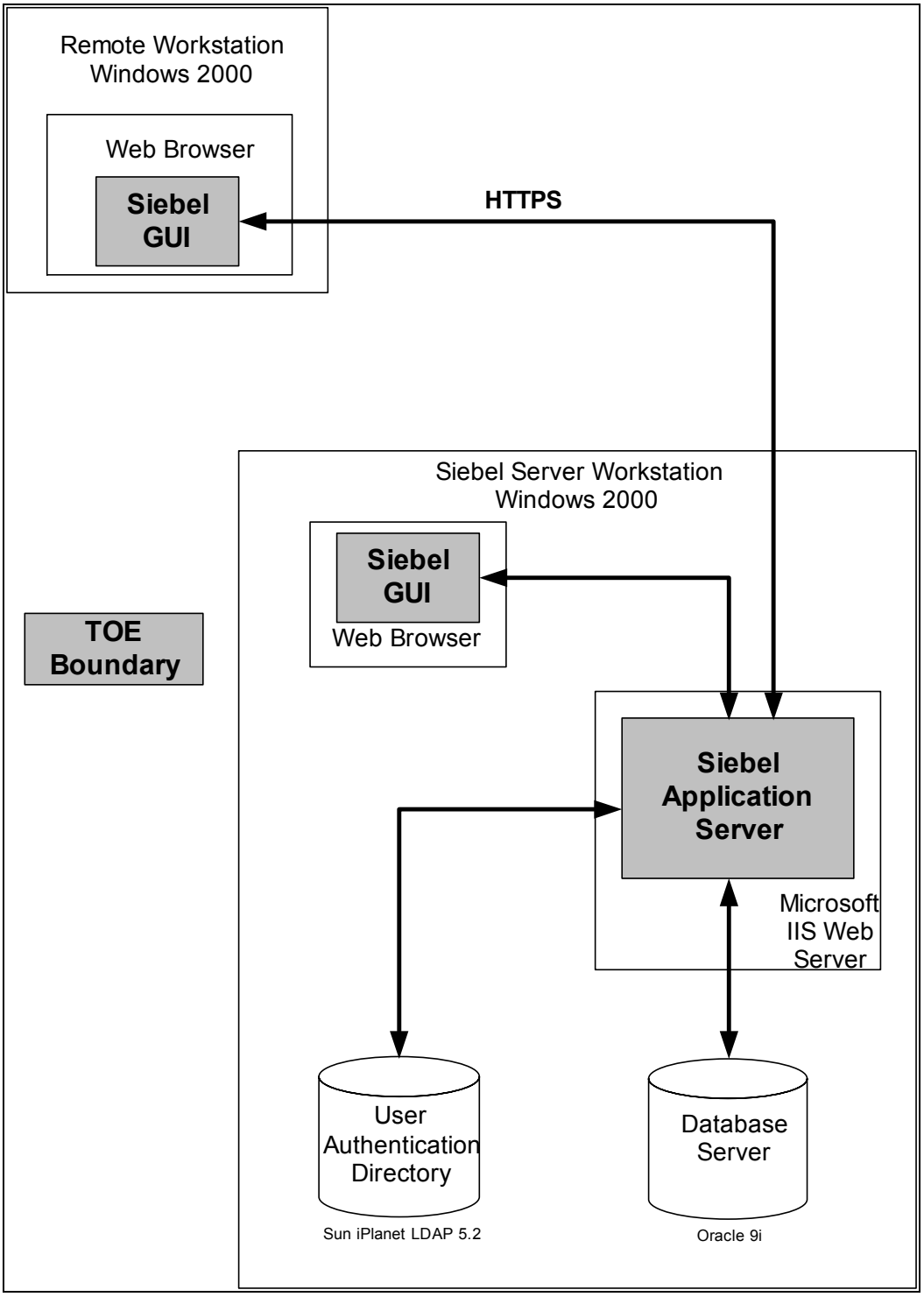

Figure 2-3 TOE Physical Boundary

2.4 Logical Scope and Boundary

Siebel eBusiness Platform provides the following security features:

- **Security audit** - Siebel eBusiness Platform provides the ability, when configured, to audit the following events: creation, deletion, generated modifications, and copying business component fields. These events include those caused by administrators or end users. TSF data is viewed as stored information in fields within a business component. Siebel eBusiness Platform provides a utility for searching, sorting, and viewing audit records. CC users will need to ensure that the audit capability is turned on according to the supplied guidance.
- **User data protection** - Siebel eBusiness Platform provides access control through the enforcement of the Siebel eBusiness Platform Access Control SFP (See Table 5-2). The Siebel eBusiness Platform Access Control SFP is based on user responsibilities as described in the Administrator's Guide.
- **Security management** - Siebel eBusiness Platform provides security management of TOE security functions and data through the use of the Administrator Interface. Through the enforcement of the Siebel eBusiness Platform Access Control SFP (Table 5-2), the ability to manage various security attributes and security functions are controlled.
- **Partial protection of TSF** - Siebel eBusiness Platform protects its programs and data from unauthorised access through its own interfaces per the Siebel eBusiness Platform Access Control SFP (Table 5-2). The TOE, after being invoked by the Operating System, protects its programs and data from unauthorized access through it's own interfaces (GUI) per the Siebel eBusiness Access Control. All other protections are handled by the Operating System (see section 2.5)

2.5 TOE Security Environment

It is assumed that there will be no untrusted users or software on the Siebel eBusiness Platform hosts and that the host will be physically protected from unauthorized tampering. Siebel eBusiness Platform is dependent upon the underlying operating system platforms to provide reliable time stamps and to protect the Siebel eBusiness Platform hosts from other interference or tampering. Siebel eBusiness Platform relies upon third-party software to provide:

- for the protection of data transfer between TOE components and for the trusted communication path between authorized account holders and the TOE (encryption software),
- for the web services needed for the GUI (web browser),
- for the TSF data storage (third-party relational database),
- for the LDAP Directory Server used for identification and authentication purposes.

The TOE security environment can be categorized as follows:

- **Cryptographic Support** – All network communications between Siebel eBusiness Platform components are encrypted. Communications between the User interface and the Siebel Application Server host are encrypted. Since third party software is used to provide confidentiality (included with the Srong Encryption Pack option), the encryption functions are not part of the TOE. The TOE relies on the IT environment to provide cryptographic support. These include:
    - encryption to prevent disclosure;

- hashing of user passwords that are stored in the database or directory;
- industry standard hashing function to support the above operations.

- **Identification and Authentication** - The IT Environment provides user identification and authentication through the use of user accounts and the enforcement of password policies. The LDAP server receives the login information from the Siebel Application Server and checks the validity of the username and password.

- **Partial Protection of TSF**

  The Siebel eBusiness Platform relies on the underlying OS to provide security capabilities for the TOE's protection. For protecting the integrity of the TOE and the TOE data, the OS Security Functional Requirements shall include domain separation and a reliable time stamp.

3 TOE Security Environment

This section identifies secure usage assumptions and threats to security. There are no organizational security policies.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Table 3-1 Assumptions

No.	Assumption	Description
1	A.Access	It is assumed that only authorized TOE, database, and operating system administrators have access to the TSF data stored in the database and the underlying operating system.
2	A.Admin	The authorized administrator is trusted to correctly configure and operate the TOE according to the instructions provided by the TOE documentation.
3	A.Manage	It is assumed that one or more authorized administrators are assigned who are competent to manage the TOE and the security of the information it contains, and who can be trusted not to deliberately abuse their privileges so as to undermine security.
4	A.No_Untrusted	It is assumed that there will be no untrusted users and no untrusted software on the Siebel eBusiness Platform Server host.
5	A.Physical	The TOE components critical to the security policy enforcement will be protected from unauthorized physical modification.
6	A.Time	It is assumed that the underlying operating system provides reliable time stamps.
7	A.Users	It is assumed that users will protect their authentication data.
8	A.Users_Pass	It is assumed that there is the capability to hash and store user passwords.

3.2 Threats

The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated, with access to standard equipment and public information.

The TOE will counter the following threats to security:

Table 3-2 Threats

No.	Threat	Description
1	T.BadPassword	A user may select a weak password, for example an easily guessable password. Thus allowing attackers to guess the user's password and obtain unauthorized access to resources and TSF data protected by the TOE.
2	T.Bypass	An attacker may bypass TOE security functions to gain unauthorized access to resources protected by the TOE.
3	T.Mismanage	Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.
4	T.Privilege	An attacker may exploit the TOE and gain unauthorized access to resources protected by the TOE.
5	T.Tamper	An attacker may attempt to modify TSF programs and data.
6	T.Transmit	TSF data may be disclosed or modified by an attacker while being transmitted between TOE components.
7	T.Undetect	Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered.

4 Security Objectives

4.1 Security Objectives for the TOE

Table 4-1 Security Objectives for TOE

No.	Objective	Description
1	O.Access	The TOE will provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the Siebel eBusiness Platform Access Control SFP.
2	O.Admin	The TOE will provide the functionality to enable an authorized administrator to effectively manage the TOE and its security functions.
3	O.Attributes	The TOE will be able to maintain subject and user security attributes.
4	O.Audit	The TOE will provide the capability to detect and create records of security-relevant events associated with users.
5	O.NonBypass	The TOE will ensure the Siebel eBusiness Access Control SFP (Table 5-2) is invoked and succeeds before each function within the TSC is allowed to proceed.
6	O.Partial_Domain_Sep	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces.
7	O.Protect_Auth	The TOE will provide protected authentication feedback during user login.
8	O.Responsibilities	The TOE will support multiple administrative responsibilities (equivalent to CC terminology of roles).

Application Note: User 'responsibilities' are 'roles' in Siebel eBusiness Platform terminology; therefore, for consistency with all Siebel documents the word 'responsibility' is used instead of 'role'.

4.2 Security Objectives for the Environment

4.2.1 Security Objectives for the IT Environment

The security objectives for the IT environment are as follows:

Table 4-2 Security Objectives for IT Environment

No.	Objective	Description
9	OE.Partial_Domain_Sep	The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces.
10	OE.Protect_Comm	The IT environment will protect communications between the TOE and its components.
11	OE.Stored_Hash_Pass	The IT environment will hash the stored passwords.
12	OE.Time	The underlying operating system will provide reliable time stamps.
13	OE.NonBypass	The IT environment will ensure that its security functions cannot be bypassed.
14	OE.ID_Auth	The IT environment will be able to identify and authenticate users prior to allowing access to authorized TOE functions and data.

4.2.2 Non-IT Security Objectives

The Non-IT security objectives are as follows:

Table 4-3 Non-IT Security Objectives

No.	Objective	Description
15	ON.Install	Those responsible for the TOE will ensure that the TOE is delivered and installed in a manner that maintains IT security.
16	ON.No_Untrusted	The authorized administrator will ensure that there are no untrusted users and no untrusted software on the Siebel eBusiness Platform Server host.
17	ON.Operations	The authorized administrator will ensure the proper procedures and guidelines in the guidance documentation are being followed and carry out during installation, configuration, managing, and operating of the TOE in a secure manner.
18	ON.Protect_Auth	The users will ensure that their authentication data is held securely and not disclosed to unauthorized persons.
19	ON.Person	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.
20	ON.Physical	Those responsible for the TOE will ensure that those parts of the TOE critical to security policy are protected from any physical attack.

5 IT Security Requirements

5.1 Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 2.2 of the Common Criteria for Information Technology Security Evaluation. Font style and clarifying information conventions were developed to aid the reader.
The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Common Criteria, Part 1, section 4.4.1.3.2 as:

- assignment: allows the specification of an identified parameter;
- refinement: allows the addition of details or the narrowing of requirements;
- selection: allows the specification of one or more elements from a list; and
- iteration: allows a component to be used more than once with varying operations.

This ST indicates which text is affected by each of these operations in the following manner:

- *Assignments* and *Selections* specified by the ST author are in **[*italicized bold text*]**.
- *Refinements* are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text***.
- *Iterations* are identified with a dash number "-#". These follow the short family name and allow components to be used more than once with varying operations. "*" refers to all iterations of a component.
- *Explicitly Stated Requirements* will be noted with a "_EXP" added to the component name.
- *Application notes* provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*
- *NIAP and CCIMB Interpretations* have been reviewed. Relevant Interpretations are included and are noted in Interpretation Notes. Interpretation Notes are denoted by *italicized text.* The original CC text modified by the interpretation is not denoted nor explained.
- *Comments* are provided as an aid to the ST author and evaluation team. These items will be deleted in the final version of the ST.

5.2 TOE Security Functional Requirements

The TOE security functional requirements are listed in Table 5-1. They are all taken from Part 2 of the Common Criteria.

Table 5-1 Functional Components

No.	Component	Component Name
1.	FAU_GEN.1	Audit data generation
2.	FAU_GEN.2	User identity association
3.	FAU_SAR.1	Audit Review
4.	FAU_SAR.2	Restricted Audit Review
5.	FAU_SAR.3	Selectable Audit Review
6.	FAU_SEL.1	Selective audit

No.	Component	Component Name
7.	FDP_ACC.2	Complete access control
8.	FDP_ACF.1	Security attribute based access control
9.	FIA_ATD.1	User attribute definition
10.	FIA_UAU.7	Protected authentication feedback
11.	FIA_USB.1	User-subject binding
12.	FMT_MOF.1	Management of security functions behaviour
13.	FMT_MSA.1*	Management of security attributes
14.	FMT_MSA.3	Static attribute initialisation
15.	FMT_MTD.1	Management of TSF data
16.	FMT_SMF.1	Specification of management functions
17.	FMT_SMR.1	Security roles
18.	FPT_RVM_EXP.1-1	Non-bypassability of the TSP
19.	FPT_SEP_EXP.1-1	TSF domain separation

5.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

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 **[*not specified*]** level of audit; and

c) the following auditable events:

[*Operations:*

- ***update to business component fields,***
- ***create new business component fields,***
- ***delete business component fields, and***
- ***copy business component fields*.]**

Application Note: The startup and shutdown of the audit function is the equivalent to the startup and shutdown of the Siebel Server. There is no way to separate the shutdown of the audit function vs the server. The startup and shutdown of the Siebel Server is logged into the system audit trail.

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

a) Date and time of the event, type of event, subject identity, and 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:

[*the following audit information:*

- ***business component,***
- ***new value,***
- ***old value,***
- ***field, and***

- ***row ID of the record being changed].***

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.2 User identity association

Hierarchical to: No other components.

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

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide **[*Siebel Administrator*]** with the capability to read **[*all audit information*]** from the audit records.

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1 The TSF shall provide the ability to perform **[*searches and sorting*]** of audit data based on **[*user identity, business component field, operations, and date*]**.

Dependencies: FAU_SAR.1 Audit review

FAU_SEL.1 Selective audit

Hierarchical to: No other components.

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

a) [*user identity and event type*]

b) [*business component and business component fields*].

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

5.2.2 Class FDP: User Data Protection

FDP_ACC.2 Complete access control

Hierarchical to: FDP_ACC.1

FDP_ACC.2.1 The TSF shall enforce the **[*Table 5-2 Siebel eBusiness Platform Access Control SFP*]** on **[*Subjects and Objects listed in Table 5-2*]** and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Dependencies: FDP_ACF.1 Security attribute based access control

Table 5-2 Siebel eBusiness Platform Access Control SFP

Application Note: User 'responsibilities' are 'roles' in Siebel eBusiness Platform terminology; therefore, for consistency we have used the word 'responsibility' instead of 'role'.

Subjects with responsibilities of the following:	Description of Access	User Data Objects:
Siebel Administrator	Full Administrative Access privileges The Siebel Administrator Account has access to all information in the application.	• Master Data • Customer Data • Other Data
Custom Administrator	Limited Administrative Access privileges The Custom Administrator Account has limited access to the security functions. The Siebel Administrator can create a custom administrator account with limited administrative access.	• Master Data • Customer Data • Other Data
Custom End User	Limited Access privileges The End User only has limited access to views and data. Access is based on view level and record level access controls.	• Master Data • Customer Data • Other Data

Application Note: A description of Master Data, Customer Data, and Other data is below:

- *Data - The type of data and whether the data is categorized determines which access control mechanisms can be applied.*
    - *Master Data - This data includes the following referential data: products, literature, solutions, resolution items, decision issues, auctions, events, training courses, and competitors. Master data can be organized into catalogs, which are hierarchies of categories.*
    - *Customer Data - This data includes contacts and transactional data such as opportunities, orders, quotes, service requests, and accounts*
    - *Other Data - This data includes referential data that is not master data, such as price lists, cost lists, rate lists, and Smartscripts.*

FDP_ACF.1 Security attribute based access control
Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the **[*Table 5-2 Siebel eBusiness Platform Access Control SFP*]** to objects based on the following: **[**

Subjects with Responsibilities of the following: (Siebel Administrator, Custom Administrator, and Custom End User):
Subject security attributes:

User identity
Responsibilities,
Organizations,
Divisions,
Positions,
Access Groups,

Objects: master data, customer data, other data
Object security attributes: none**]**.
FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[**

1. ***The Siebel administrator, custom administrator, and end user may view pages, features, and functions through the Graphical User Interface and perform actions associated with their responsibilities,***
2. ***Responsibilities - Every user has one or more responsibilities, which define the collection of views to which the user has access. If a particular view is not in a user's responsibilities, then the user does not see that view.***
3. ***Individual data can be associated with a user identity. The Siebel Administrator can restrict access to the data to that person. Typically, personal access control can be implemented when data has a creator or a person is assigned to the data, usually as the owner.***
4. ***Users can also be associated with one or more positions. Every position is associated with a division. The position is then also automatically associated with one organization, the organization with which the division is associated. The user can only log into one position at any time, so the user is automatically associated with one division and one organization at a time—the division and organization associated with the position.***
5. ***If a user has been assigned as a custom administrator, the user has the access permissions that have been assigned to this account.***
6. ***Master data can be organized into catalogs and hierarchical categories. A catalog can be thought of as the name for an entire hierarchy of categories. Individual data items are contained in categories. A category can contain one or more types of master data. A category can be a node in only one catalog. A data item can exist in one or more categories, in one or more catalogs. A catalog can be public or private. If it is private, some access control is applied at the catalog level. If it is public, then all users can see this catalog, but not necessarily categories within this catalog, depending on whether the categories are private or public.***
7. ***Siebel administrators can create responsibilities to further increase the usability of Siebel applications. When you create responsibilities and assign users to these***

responsibilities by default, users only see the screen tabs and view tabs for their responsibilities.

8. ***Access groups are an assigned attribute that controls access by groups to categorized master data. An access group is a collection of any combination of positions, organizations, and divisions. Its members cannot be individual user identities.*** **]**

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

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

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

5.2.3 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

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

- **[*User Identity,***
- ***Responsibilities (see column 1 of Table 5-2),***
- ***Organizations,***
- ***Divisions,***
- ***Positions,***
- ***Access Groups.*****]**

Dependencies: No dependencies.

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1 The TSF shall provide only **[*a display of the typed in user name and asterisks for the password for password-based authentication*]** to the user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

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

Dependencies: FIA_ATD.1 User attribute definition

5.2.4 Class FMT: Security Management

FMT_MOF.1 Management of Security Functions Behaviour

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to **[*determine the behaviour of, disable, enable, and modify the behaviour*]** of the functions **[*related to the selection of auditable events (see FAU_SEL.1.1) and audit function (see FAU_GEN.1.1)*]** to **[*the Siebel Administrator*].**

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

FMT_MSA.1-1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1-1 The TSF shall enforce the **[*Table 5-2 Siebel eBusiness Platform Access Control*]** to restrict the ability to **[*query, modify, delete,* [*create, and rename*]]** the security attributes **[*user identity*]** to **[*the Siebel Administrator*]**.

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

FMT_MSA.1-2 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1-2 The TSF shall enforce the **[*Table 5-2 Siebel eBusiness Platform Access Control*]** to restrict the ability to **[*query, modify, delete,* [**or** *create*]]** the security attributes **[*responsibilities and access groups*]** to **[*the Siebel Administrator*]**.

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

FMT_MSA.1-3 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1-3 The TSF shall enforce the **[*Table 5-2 Siebel eBusiness Platform Access Control*]** to restrict the ability to **[*change_default*, *query, modify,* [*or create*]]** the security attributes **[*organization*]** to **[*the Siebel Administrator*]**.

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

FMT_MSA.1-4 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1-4 The TSF shall enforce the **[*Table 5-2 Siebel eBusiness Platform Access Control SFP*]** to restrict the ability to **[*query, modify,* [*or create*]]** the security attributes **[*divisions*]** to **[*the Siebel Administrator*]**.

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

FMT_MSA.1-5 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1-5 The TSF shall enforce the **[*Table 5-2 Siebel eBusiness Platform Access Control SFP*]** to restrict the ability to **[*query, modify,* [*rename, or create*]]** the security attributes **[*positions*]** to **[*the Siebel Administrator*]**.

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the **[*Table 5-2 Siebel eBusiness Platform Access Control SFP*]** to provide **[*restrictive*]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **[*Siebel Administrator*]** to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to **[*change_default, query, modify, delete,* [*create*]] *as specified in Table 5-3*]** the **[*TSF Data as specified in Table 5-3*]** to **[*the responsibilities as specified in Table 5-3*]*.***

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

Table 5-3 Management of TSF Data

Application Note: User 'responsibilities' are 'roles' in Siebel eBusiness Platform terminology; therefore, for consistency we have used the word 'responsibility' instead of 'role'.

Subjects with responsibilities of the following:	Allowed Operations on TSF Data (Management Functions)
Siebel Administrator	The Siebel Administrator can: • Select auditable events and review the audit logs • Query, modify, delete, create, and rename user identities used for authentication and login information. • Add users to specified organizations • Query, modify, delete, or create responsibilities • Change_default, query, modify, or create organization(s) • Query, modify, create divisions • Query, modify, rename, or create positions • Query, modify, delete, or create access groups
Custom Administrator	This depends on the assigned view level and record level access that has been assigned this account.
Custom End User	This depends on the assigned view level and record level access that has been assigned this account.

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

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

- ***determine the behaviour of, disable, enable, and modify the behaviour of the functions related to the selection of which events are to be audited (see FAU_SEL.1.1) and audit (see FAU_GEN.1.1] (see FMT_MOF.1),***
- ***query, modify, delete, create, and rename the security attributes user identity (see FMT_MSA.1-1),***
- ***query, modify, delete, or create the security attributes responsibilities and access groups (see FMT_MSA.1-2),***
- ***change_default, query, modify, or create the security attributes organization (see FMT_MSA.1-3),***
- ***query, modify, or create the security attributes divisions, and responsibilities, (see FMT_MSA.1-4),***
- ***query, modify, rename, or create the security attributes positions (FMT_MSA.1-5),***
- ***change_default, query, modify, delete, create as specified in Table 5-3 the TSF Data as specified in Table 5-3 (See FMT_MTD.1)*****]**.

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles **[*See column 1 of Table 5-2*].**

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

Dependencies: FIA_UID.1 Timing of identification

Application Note: CC requires the use of the word 'roles' in the context of defining this SFR. Remember that user 'responsibilities' are 'roles' in Siebel eBusiness Platform terminology.

5.2.5 Class FPT: Protection of the TOE Security Functions

FPT_RVM_EXP.1-1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM_EXP.1.1-1 The TSF, when invoked by the underlying host OS, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP_EXP.1-1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP_EXP_1.1-1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

FPT_SEP_EXP_1.2-1 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

5.2.6 Strength of Function

The overall strength of function requirement is SOF-Basic.

5.3 Security requirements for the IT Environment

The functional security requirements for the IT Environment consist of the following components derived from Part 2 of the CC, International interpretations, NIAP interpretations, and explicit components, summarized in Table 5-4 below.

Siebel eBusiness Platform requires that the operating system platform provide reliable time stamps.

Siebel eBusiness Platform requires that the operating system provides non-bypassability of the TSP and TSF domain separation.

The LDAP Directory Server is used for identification and authentication purposes.

End-to-end encryption protects confidentiality along the entire data path: from the client browser, to the Web server, to the Siebel application server, to the database. Since third party software is used to provide confidentiality, the encryption functions are not part of the TOE.

Table 5-4 Functional Components for the IT environment

No.	Component	Component Name

No.	Component	Component Name
20.	FCS_CKM.1*	Cryptographic key generation
21.	FCS_CKM.4	Cryptographic key destruction
22.	FCS_COP.1*	Cryptographic operation
23.	FIA_UAU.2	User authentication before any action
24.	FIA_UID.2	User identification before any action
25.	FMT_MSA.2	Secure security attributes
26.	FPT_RVM_EXP.1-2	Non-bypassability of the TSP
27.	FPT_SEP_EXP.1-2	TSF domain separation
28.	FPT_STM.1	Reliable Time Stamps
29.	FPT_ITC.1	Inter-TSF confidentiality during transmission

5.3.1 Class FCS: Cryptographic Support

FCS_CKM.1-1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1-1 **Refinement:** The ***IT environment*** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[*AES*]** and specified cryptographic key sizes **[56, *128, 192, 256 bit*]** that meet the following: **[*Advanced Encryption Standard (AES), FIPS PUB 197*]**.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.1-2 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1-2 **Refinement:** The ***IT environment*** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[*RSA*]** and specified cryptographic key sizes **[*1024 bits*]** that meet the following: **[*ANSI X9.31*;*Digital Signature Standard (DSS), FIPS PUB 186-2*]**.

Dependencies: [FCS_CKM.2 Cryptographic key distribution
or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1 **Refinement:** The ***IT environment*** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[*which zeroizes all plaintext cryptographic keys*]** that meets the following: **[*none*]**.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FCS_CKM.1 Cryptographic key generation]
FMT_MSA.2 Secure security attributes

FCS_COP.1-1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1-1 **Refinement:** The ***IT environment*** shall perform **[*symmetric key encryption and decryption*]** in accordance with a specified cryptographic algorithm **[*AES*]** and cryptographic key sizes **[56, *128, 192, 256 bit*]** that meet the following: **[*Advanced Encryption Standard (AES), FIPS PUB 197*]**.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_COP.1-2 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1-2 **Refinement:** The ***IT environment*** shall perform **[*hashing functions of the user passwords that are stored in the database or directory*]** in accordance with a specified cryptographic algorithm **[*SHA-1*]** and cryptographic key sizes **[*80 bit*]** that meet the following: **[*Secure Hash Standard (SHS), FIPS PUB 180-2*]**.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.3.2 Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

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

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1 **Refinement:** The ***IT environment*** shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

5.3.3 Class FMT: Security Management

FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

FMT_MSA.2.1 **Refinement:** The ***IT environment*** shall ensure that only secure values are accepted for security attributes.

Dependencies: ADV_SPM.1 Informal TOE security policy model
[FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

5.3.4 Class FPT: Protection of the TOE Security Functions

FPT_ITC.1 Inter-TSF confidentiality during transmission

Hierarchical to: No other components.

FPT_ITC.1.1 **Refinement:** The ***IT environment*** shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission.

Dependencies: No dependencies

FPT_RVM_EXP.1-2 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM_EXP.1.1-2 The IT environment shall ensure that Operating System Security Policy enforcement functions are invoked and succeed before each function within the Operating System's Scope of Control is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP_EXP.1-2 TSF domain separation

Hierarchical to: No other components.

FPT_SEP_EXP1.1-2 The IT environment shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through the Operating System's Interface.

FPT_SEP_EXP.1.2-2 The IT environment shall enforce separation between the security domains of subjects in the Operating System's Scope of Control.

Dependencies: No dependencies

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 **Refinement:** The ***IT environment*** shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies

5.4 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2) taken from Part 3 of the Common Criteria. None of the assurance components is refined. The assurance components are listed in Table 5-5 EAL2 Assurance Components.

Table 5-5 EAL2 Assurance Components

Component	Component Title
ACM_CAP.2	Configuration items
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.1	Descriptive high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance

AGD_USR.1	User guidance
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

6 TOE Summary Specification

6.1 IT Security Functions

6.1.1 Overview

The following sections describe the IT Security Functions in each of the Siebel eBusiness Platform components.

Table 6-1 Security Functional Requirements mapped to Security Functions

SFRs	Security Class	Security Functions	Sub-functions
FAU_GEN.1	Security audit	Security Audit	AI-SA-1
			AI-SA-2
FAU_GEN.2	Security audit	Security Audit	AI-SA-3
FAU_SAR.1	Security audit	Security Audit	AI-SA-4
			AI-SA-5
FAU_SAR.2	Security audit	Security Audit	AI-SA-6
FAU_SAR.3	Security audit	Security Audit	AI-SA-7
FAU_SEL.1	Security audit	Security Audit	AI-SA-8
FDP_ACC.2	User data protection	Manage User Access	AI-MUA-1
FDP_ACF.1	User data protection	Manage User Access	AI-MUA-1
FIA_ATD.1	Identification and authentication	Manage User Access	AI-MUA-2
FIA_UAU.7	Identification and authentication	User Login	AI-UL-1
FIA_USB.1	Identification and authentication	User Login	AI-MUA-3
FMT_MOF.1	Security management	Security Management	AI-SM-1
FMT_MSA.1-1	Security management	Security Management	AI-SM-2
FMT_MSA.1-2	Security management	Security Management	AI-SM-3
FMT_MSA.1-3	Security management	Security Management	AI-SM-4
FMT_MSA.1-4	Security management	Security Management	AI-SM-5
FMT_MSA.1-5	Security management	Security Management	AI-SM-6
FMT_MSA.3	Security management	Security Management	AI-SM-7
FMT_MTD.1	Security management	Security Management	AI-SM-8
FMT_SMF.1	Security management	Security Management	AI-SM-9
FMT_SMR.1	Security management	Security Management	AI-SM-10
FPT_RVM_EXP.1-1	Protection of the TSF	Manage User Access	AI-MUA-4
FPT_SEP_EXP.1-1	Protection of the TSF	Manage User Access	AI-MUA-5

6.1.2 Siebel eBusiness Platform

6.1.2.1 Security Audit Function

Siebel eBusiness Platform provides the security audit function. To maintain data continuity and monitor activity on a Siebel site, the TSF can maintain an audit trail of information that indicates when business component fields have been changed, who made the change, and what has been changed. The Security Audit Function is configurable and creates a history of the changes that have been made to various types of information in various Siebel applications. An audit trail is a record showing who has accessed an item, which

operation was performed, when it was performed, and how the value was changed. Therefore, it is useful for maintaining security, examining the history of a particular record, and documenting modifications for future analysis and record keeping. Audit Trail logs information without requiring any interaction with, or input from users. By using the Audit Trail, users can track which user identity modified a certain field and what data has been changed.

The Graphical User Interface supports the following choice of audit trail modes:

- File auditing. An audit trail can be written to files and later imported into the database, providing better performance.
- Database auditing. An audit trail can be written directly into the database, supporting both remote users and replicated databases. Changes to an audit trail field are cached in the application. Exiting from the Siebel application and restarting it writes all cached changes to the database. Alternatively, when the cache size is reached, all cached entries are automatically written to the database even without exiting from the application. The evaluated configuration will be set up for database auditing.

The Siebel Administrator is able to configure and activate the Security Audit Function from the Graphical User Interface.

Table 6-2 Security Audit Function

Security Function: Security Audit Function	
Sub-function ID	Sub-function description
AI-SA-1	Siebel eBusiness Platform generates the following types of audit events: • startup and shutdown of audit functions, Operations: • update to business component fields, • create new business component fields, • delete business component fields, and • copy business component fields. (FAU_GEN.1.1)
AI-SA-2	Siebel eBusiness Platform records the information for all events: • Date and time of event, • Type of event, • Subject identity, • Success or failure of event, • business component, • new value, • old value, • field, and • row ID of the record being changed (FAU_GEN.1.2)
AI-SA-3	Siebel eBusiness Platform will associate each auditable event with the identity of the user that caused the event. The user is identified by the user identity of the logged in user of the TOE. (FAU_GEN.2)

Security Function: Security Audit Function	
Sub-function ID	Sub-function description
AI-SA-4	Siebel eBusiness Platform provides the Siebel administrator with the capability to read all audit information from the audit records. The Siebel Administrator can query Audit Trail information in the Audit Trail Items view. (FAU_SAR.1.1)
AI-SA-5	Siebel eBusiness Platform provides the audit records in a manner suitable for the user to interpret the information. The Siebel Administrator can query Audit Trail information in the Audit Trail Items view. (FAU_SAR.1.2)
AI-SA-6	Siebel eBusiness Platform prohibits all users read access to the audit records, except those that have been granted explicit read access. (FAU_SAR.2)
AI-SA-7	Siebel eBusiness Platform provides the ability to perform searches and sorting of the audit data based on user identity, business component field, dates, or operations. The Siebel Administrator can query Audit Trail information in the Audit Trail Items view. (FAU_SAR.3)
AI-SA-8	Siebel eBusiness Platform is able to include or exclude auditable events from the set of audited events based on specific attributes: user identity, event type, business component, and business component fields. These can be managed through the Graphical User Interface. (FAU_SEL.1)

6.1.2.2 Manage User Access Function

Siebel eBusiness Platform provides the manage user access function. The manage user access function provides access control through the enforcement of the Siebel eBusiness Platform Access Control SFP Policy. The Siebel eBusiness Platform Access Control SFP is based on user responsibilities in the Administrator's Guide. This functionality is specified using security attributes in user records in the Siebel eBusiness Platform Data Store.

Several different access control mechanisms can be used to associate data with users. Access control mechanisms include user identity, responsibilities, organizations, divisions, positions, and access groups—each provide a slightly different set of functions. Access control is the means to control visibility of and access to data records to each individual user. In Siebel application terms, a screen is a collection of views. The screen represents a broad area of functionality, such as working with accounts. To the user, a view is simply one Web page. Within a view, the user may see and access lists of data records or forms presenting individual records. Siebel access control consists of the following:

1. The Siebel administrator, custom administrator, and end user may view pages, features, and functions through the Graphical User Interface and perform actions associated with their responsibilities,
2. Responsibilities - Every user has one or more responsibilities, which define the collection of views to which the user has access. If a particular view is not in a user's responsibilities, then the user does not see that view.
3. Individual data can be associated with a user identity. The Siebel Administrator can restrict access to the data to that person. Typically, personal access control can be implemented when data has a creator or a person is assigned to the data, usually as the owner.
4. Users can also be associated with one or more positions. Every position is associated with a division. The position is then also automatically associated with one organization, the organization with which the division is associated. The user can only log into one position at any time, so the user is automatically associated with one division and one organization at a time—the division and organization associated with the position.
5. If a user has been assigned as a custom administrator, the user has the access permissions that have been assigned to this account.

6. Master data can be organized into catalogs and hierarchical categories. A catalog can be thought of as the name for an entire hierarchy of categories. Individual data items are contained in categories. A category can contain one or more types of master data. A category can be a node in only one catalog. A data item can exist in one or more categories, in one or more catalogs. A catalog can be public or private. If it is private, some access control is applied at the catalog level. If it is public, then all users can see this catalog, but not necessarily categories within this catalog, depending on whether the categories are private or public.
7. Siebel administrators can create responsibilities to further increase the usability of Siebel applications. When you create responsibilities and assign users to these responsibilities by default, users only see the screen tabs and view tabs for their responsibilities.
8. Access groups are an assigned attribute that controls access by groups to categorized master data. An access group is a collection of any combination of positions, organizations, and divisions. Its members cannot be individual user identities.

The Siebel access control mechanisms include filtering of available views based on the user's identity and responsibilities. The user's identity and responsibilities define the collection of views to which the user has access.

The Siebel access control mechanisms include controlling access to objects based on the user's position and organization. A position can relate to a job title in an organization. Positions provide an appropriate basis for access control in many scenarios because a position in an organization is typically more stable than the individual's assignment to the position (ie. project manager). Customer data and some types of referential data can be associated with one or more positions. A user is associated with one organization at any given time, the organization to which the user's active position belongs.

The Siebel access control mechanisms include controlling access to objects based on the user's access group. Access group access control is a means to control access by groups to categorized master data. An access group is a collection of any combination of positions, organizations, and divisions. Its members cannot be individual user identities. A user is associated with an access group if, during the current session, the user is associated with a position, organization, and division that is a member of the access group. The Siebel Administrator can create hierarchies of access groups. An access group can belong to only one access group hierarchy. That is, an access group can have only one parent access group. For example, the access group mentioned above might belong to a hierarchy of access groups for the purpose of granting differing levels of access to sales tools. The Siebel Administrator can grant access groups access to catalogs and categories of master data.

Non-bypassability of the TSP

The TSF after being invoked by the OS ensures that TOE security functions are non-bypassable. Siebel ensures that security protection enforcement functions are invoked and succeed before each function within Siebel's scope of control is allowed to proceed. All management user operations are conducted in the context of an associated management session. This management session is allocated only after successful authentication into the TOE. User operations are checked for conformance to the granted level of access, and rejected if not conformant. The management session is destroyed when the corresponding user logs out of that session.

Domain Separation

Siebel maintains a security domain for its own execution and enforces separation between the security domains of users initiating actions through its own user interface.

The TSF maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects. Siebel Server is a passive device in that it indirectly connects to networks via other devices' e.g. network interface.

Siebel's protected domain includes the Siebel software and all of its software components.

The TSF enforces separation between the security domains of subjects in the TSC. Siebel maintains separation between data from different input interfaces.

Siebel relies partially on the Operating System to provide file access permissions and identification and authentication of users at the OS level The Siebel Access Control Policy is providing protection to accessing these files. The underlying assumption regarding the operation of Siebel is that it is maintained in a physically secure environment.

Table 6-3 Manage User Access Function

Security Function: Manage User Access Function	
Sub-function ID	Sub-function description
AI-MUA-1	Siebel eBusiness Platform enforces the Siebel eBusiness Platform Access Control SFP (See Table 5-2 Siebel eBusiness Platform Access Control) (FDP_ACC.2) (FDP_ACF.1)
AI-MUA-2	Siebel eBusiness Platform maintains the following information for each user: user identity, responsibilities, organizations, divisions, positions, and access groups. (FIA_ATD.1)
AI-MUA-3	Siebel eBusiness Platform associates all user security attributes with subjects acting on behalf of that user. The security attributes relate to access control rules. (FIA_USB.1)
AI-MUA-4	Siebel eBusiness Platform ensures that the Table 5-2 Siebel eBusiness Platform Access Control is invoked and succeeds before each function is allowed to proceed. (FPT_RVM_EXP.1-1)
AI-MUA-5	Siebel eBusiness Platform maintains a security domain for its own execution and enforces separation between security domains of users actions through its own TSFI. (FPT_SEP_EXP.1-1)

6.1.2.3 Security Management Function

Siebel eBusiness Platform provides the security management function through the use of the Graphical User Interface. Through the enforcement of the Siebel eBusiness Platform Access Control SFP, the ability to manage various security attributes and TSF data is controlled.

The Siebel eBusiness Platform enables administrators to control access to information based on a set of explicitly defined user responsibilities, the user's relationship to the data, and access groups.

Table 6-4 Security Management Function

Security Function: Security Management Function	
Sub-function ID	Sub-function description
AI-SM-1	The Siebel eBusiness Platform restricts the ability to determine the behaviour of, disable, enable, and modify the behaviour of the functions related to the selection of auditable events (see FAU_SEL.1.1) and the audit function (see FAU_GEN.1.1) to the Siebel Administrator. (FMT_MOF.1)
AI-SM-2	The Siebel eBusiness Platform restricts the ability to query, modify, delete, create, and rename the user identity attributes to the Siebel Administrator. (FMT_MSA.1-1)

Security Function: Security Management Function	
Sub-function ID	Sub-function description
AI-SM-3	Siebel eBusiness Platform restricts the ability to query, modify, delete, or create the responsibility and access group attributes to the Siebel Administrator. (FMT_MSA.1-2)
AI-SM-4	Siebel eBusiness Platform restricts the ability to change_default, query, modify, or create the organization attribute to the Siebel Administrator. (FMT_MSA.1-3)
AI-SM-5	Siebel eBusiness Platform restricts the ability to query, modify, or create the divisions attribute to the Siebel Administrator. (FMT_MSA.1-4)
AI-SM-6	Siebel eBusiness Platform restricts the ability to query, modify, rename, or create the positions attribute to the Siebel Administrator. (FMT_MSA.1-5)
AI-SM-7	Siebel eBusiness Platform provides restrictive default values for security attributes as specified in Table 5-2 Siebel eBusiness Platform Access Control and allows the Siebel Administrator to specify alternative initial values. (FMT_MSA.3)
AI-SM-8	Siebel eBusiness Platform restricts the ability to access data as specified in Table 5-2 Siebel eBusiness Platform Access Control . Also refer to Table 5-3 Management of TSF Data to view the allowed operations on TSF data. (FMT_MTD.1)
AI-SM-9	Siebel eBusiness Platform provides the following security management functions: • determine the behaviour of, disable, enable, and modify the behaviour of the functions related to the selection of which events are to be audited (see FAU_SEL.1.1) and audit (see FAU_GEN.1.1) (see FMT_MOF.1), • query, modify, delete, create, and rename the user identity security attribute (see FMT_MSA.1-1), • query, modify, delete, or create the responsibility and access group security attributes (see FMT_MSA.1-2), • change_default, query, modify, or create the organization security attribute (see FMT_MSA.1-3), • query, modify, or create the divisions security attribute (see FMT_MSA.1-4), • query, modify, rename, or create the positions security attribute (FMT_MSA.1-5), • change_default, query, modify, delete, create as specified in Table 5-3 the TSF Data as specified in Table 5-3. (See FMT_MTD.1)]. (FMT_SMF.1)
AI-SM-10	Siebel eBusiness Platform maintains the responsibilities (roles): • See Table 5-2 in section 5.2 (FMT_SMR.1)

6.1.2.4 User Login Function

Table 6-5 User Login Function

Security Function: User Login Function	
Sub-function ID	Sub-function description
AI-UL-1	The Siebel eBusiness Platform Graphical User Interface provides only a display of the typed in user name and asterisks for the password when password authentication is used. (FIA_UAU.7)

6.1.3 SOF Claims

The threat level for the TOE authentication function is assumed to be SOF-basic. This defines a level of authentication strength of function where analysis shows that the function provides basic protection against straightforward or intentional breach of TOE security by attackers possessing a minimum attack potential. The overall SOF is SOF-basic.

6.2 Assurance Measures

The Siebel eBusiness Platform satisfies the assurance requirements for Evaluation Assurance Level (EAL)2. The following items are provided as evaluation evidence to satisfy the EAL2 assurance requirements:

Table 6-6 Assurance Measures

Security Assurance Requirement	**How Satisfied**
ACM_CAP.2	July 2003: New Siebel Version Numbering Scheme
ADO_DEL.1	RMR_MR Process – QE Release Perspective v2.2
	Document titled: Building Product Kits
ADO_IGS.1	Siebel eBusiness Applications ADO_DEL.1 Document November 2005
	SIEBEL SHIPPING PROCESS
ADV_FSP.1	Siebel eBusiness Applications Administration Guide v7.8, Rev A
	Siebel eBusiness Security Guide for eBusiness Applications v7.8 Rev A
	Siebel System Administration Guide V7.8
	Siebel eBusiness Securing Siebel eBusiness Applications (Hardening Guide)
	Siebel eBusiness Platform FSP v1.3.doc
ADV_HLD.1	ADV_HLD v9.doc
ADV_RCR.1	ADV_RCR Specification v1.1.doc
AGD_ADM.1	Siebel eBusiness Applications Administration Guide v7.5
	Siebel eBusiness Security Guide for eBusiness Applications v7.5
	Siebel eBusiness Platform v7.5
	Siebel eBusiness Securing Siebel eBusiness Applications (Hardening Guide)
AGD_USR.1	Siebel eBusiness Applications Administration Guide v7.8, Rev A
ATE_COV.1	Siebel Test Coverage Analysis V1.0

Security Assurance Requirement	How Satisfied
ATE_FUN.1	Siebel Test Plan and Report v2.0 with Test Cases.
ATE_IND.2	TOE for Testing
AVA_SOF.1	N/A
AVA_VLA.1	Siebel Vulnerability Analysis V 1.0

7 PP Claims

The Siebel eBusiness Platform Security Target was not written to address any existing Protection Profile.

8 Rationale

8.1 Security Objectives Rationale

8.1.1 Threats to Security

Table 8-1 shows that all the identified threats to security are countered by Security Objectives for the TOE.

Table 8-1 All Threats to Security Countered

Item	Threat Name	Security Objective
1	T.BadPassword	O.Protect_Auth
2	T.Bypass	O.NonBypass OE.NonBypass
3	T.Mismanage	O.Access O.Admin O.Audit O.Responsibilities ON.Person ON.Operations
4	T.Privilege	O.Access O.Attributes ON.Install O.Partial_Domain_Sep OE.Partial_Domain_Sep OE.ID_Auth O.Protect_Auth
5	T.Tamper	O.Partial_Domain_Sep OE.Partial_Domain_Sep O.Responsiblities O.Admin ON.Person ON.Operations
6	T.Transmit	OE.Protect_Comm
7	T.Undetect	O.Audit OE.Time

T.BadPassword: A user may select a weak password, for example an easily guessable password. Thus allowing attackers to guess the user's password and obtain unauthorized access to resources and TSF data protected by the TOE. T.BadPassword is countered by:

- O.Protect_Auth: The TOE will provide protected authentication feedback during user login. When an authorized user is typing in their password only asterisks will be seen on the screen. This will limit the ability to see what an authorized user's password is.

T.Bypass: An attacker may bypass TOE security functions to gain unauthorized access to resources protected by the TOE. T.Bypass is countered by:

- O.NonBypass: The TOE will ensure the TOE's access control policy (Table 5-2) is invoked and succeeds before allowing another TOE function to proceed. This objective counters this threat by ensuring the TOE's protection mechanisms cannot be bypassed, which requires that TSF security functions not be bypassable.
- OE.NonBypass: The IT environment will ensure that its security functions cannot be bypassed. This objective for the IT environment counters this threat by ensuring the security functions of the Operating System that support the TSF are not compromised.

T.Mismanage: Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE. T.Mismanage is countered by:

- O.Access: The TOE will provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the Siebel eBusiness Platform Access Control SFP. This objective builds upon the OE.ID_Auth objective by only permitting authorized users to access specific TOE functions. This objective provides for access controls that limit the actions an individual is authorized to perform. Requiring all accesses to the TOE to conform to a specified access control policy should reduce the risk of an unauthorized user of having full access to all TOE functions.
- O.Admin: The TOE will provide the functionality to enable an authorized administrator to effectively manage the TOE and its security functions. Administrative tools make it easier for administrators to correctly manage the TOE.
- O.Audit: The TOE will provide the capability to detect and create records of security-relevant events associated with users. This objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions. The administrator's errors would be in the audit records.
- O.Responsibilities: The TOE will support multiple administrative responsibilities (roles). Multiple administrative responsibilities can be used to enforce separation of duty, so that one authorized administrator can catch errors made by another authorized administrator.
- ON.Person: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system. This objective provides for competent personnel to administer the TOE. Well trained administrators are less likely to make administrative errors.
- ON.Operations: The authorized administrator will ensure the proper procedures and guidelines in the guidance documentation are being followed and carry out during installation, configuration, managing, and operating of the TOE in a secure manner. The procedures will provide guidance to the authorized administrator on how to securely install, configure, manage, and operate the TOE. This objective provides for operation procedures to be in place.

T.Privilege: An attacker may exploit the TOE and gain unauthorized access to resources protected by the TOE. T.Privilege is countered by:

- O.Access: The TOE will provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the Siebel eBusiness Platform Access Control SFP. This objective builds upon the OE.ID_Auth objective by only permitting authorized users to access specific TOE functions. This objective provides for access controls that limit the actions an individual is authorized to perform. Requiring all accesses to the TOE to conform to a specified access control policy should reduce the risk of an unauthorized user of having full access to all TOE functions.
- O.Attributes: The TOE will be able to maintain subject and user security attributes. This objective counters this threat by requiring the TOE to maintain attributes. These attributes associate users with user accounts and privileges that the Siebel eBusiness Access Control Policy is based on. In

addition, these attributes associate subjects with responsibilities that the Siebel eBusiness Access Control Policy is based on.

- ON.Install: Those responsible for the TOE will ensure that the TOE is delivered and installed in a manner that maintains IT security. Installing the TOE in a manner that maintains IT security includes correctly configuring the TOE. As part of installing the TOE, the TOE will be properly configured. This objective provides for secure installation and configuration of the TOE.
- O.Partial_Domain_Sep: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. The TOE will maintain separation between code executing on behalf of different users. This objective addresses this threat by providing TOE self-protection and separation between users.
- OE.Partial_Domain_Sep: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. This objective addresses this threat by protecting the TOE and its data.
- OE.ID_Auth: The IT environment will be able to identify and authenticate users prior to allowing access to authorized TOE functions and data. This objective provides for authentication of users prior to any TOE function access.
- O.Protect_Auth: The TOE will provide protected authentication feedback during user login. When an authorized user is typing in their password only asterisks will be seen on the screen. This will limit the ability to see what an authorized user's password is.

T.Tamper: An attacker may attempt to modify TSF programs and data. T.Tamper is countered by:

- O.Partial_Domain_Sep: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. The TOE will maintain separation between code executing on behalf of different users. This objective addresses this threat by providing TOE self-protection and separation between users.
- OE.Partial_Domain_Sep: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. This objective addresses this threat by protecting the TOE and its data.
- O.Responsibilities: The TOE will support multiple administrative responsibilities (roles). Multiple administrative responsibilities can be used to enforce separation of duty, so that one authorized administrator can catch errors made by another authorized administrator. In addition, having multiple administrative responsibilities will reduce the risk of an unauthorized user of having full access to all TOE functions.
- O.Admin: The TOE will provide the functionality to enable an authorized administrator to effectively manage the TOE and its security functions. Administrative tools make it easier for administrators to correctly manage the TOE.
- ON.Person: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system. This objective provides for competent personnel to administer the TOE. Carefully selected and trained administrators are less to abuse their privileges.
- ON.Operations: The authorized administrator will ensure the proper procedures and guidelines in the guidance documentation are being followed and carry out during installation, configuration, managing, and operating of the TOE in a secure manner. The procedures will provide guidance to the authorized administrator on how to securely operate the TOE. This objective provides for operation procedures to be in place.

T.Transmit: TSF data may be disclosed or modified by an attacker while being transmitted between TOE components. T.Transmit is countered by:

- OE.Protect_Comm: The IT environment will protect communications between the TOE components. This objective prevents data from being disclosed or modified when it is being transmitted between

TOE components. This threat arises when the TSF data is being transmitted between TOE Components and therefore is not within the scope of the TOE security control and protection.

T.Undetect: Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered. T.Undetect is countered by:

- O.Audit: The TOE will provide the capability to detect and create records of security-relevant events associated with users. This objective records attempts to violate the security policy.
- OE.Time: The underlying operating system will provide reliable time stamps. This objective provides for a reliable way to correlate audit records to reconstruct a potential compromise.

8.1.2 Assumptions

Table 8-2 is included as a consistency check that all security objectives for the IT environment or Non-IT security objectives map to corresponding threats and assumptions.

Table 8-2 Reverse Mapping of Security Objectives for the Environment to Threats and Assumptions

No.	Objective Name	Threat/Policy/Assumption
9	OE.Partial_Domain_Sep	T.Privilege T.Tamper
10	OE.Protect_Comm	T.Transmit
11	OE.Stored_Hash_Pass	A.Users_Pass
12	OE.Time	A.Time T.Undetect
13	OE.NonBypass	T.Bypass
14	OE.ID_Auth	T.Privilege
15	ON.Install	A.Admin T.Privilege
16	ON.No_Untrusted	A.Access A.No_Untrusted
17	ON.Operations	A.Admin T.Tamper T.Mismanage
18	ON.Protect_Auth	A.Users
19	ON.Person	A.Manage A.Admin T.Tamper T,Mismanage
20	ON.Physical	A.Physical

Table 8-3 All Assumptions Addressed

Item	Name	Objective
1	A.Access	ON.No_Untrusted
2	A.Admin	ON.Install ON.Operations ON.Person

3	A.Manage	ON.Person
4	A.No_Untrusted	ON.No_Untrusted
5	A.Physical	ON.Physical
6	A.Time	OE.Time
7	A.Users	ON.Protect_Auth
8	A.Users_Pass	OE.Stored_Hash_Pass

A.Access: It is assumed that only authorized TOE, database, and operating system administrators have access to the TSF data stored in the database and the underlying operating system. A.Access is covered by:

- ON.No_Untrusted: The authorized administrator will ensure that there are no untrusted users and no untrusted software on the Siebel eBusiness Platform Server host. This objective provides for the protection of the data store and operating system which the TOE relies on from the unauthorized access of untrusted software or users.

A.Admin: The authorized administrator is trusted to correctly configure and operate the TOE according to the instructions provided by the TOE documentation. A.Admin is covered by:

- ON.Install: Those responsible for the TOE will ensure that the TOE is delivered and installed in a manner that maintains IT security. Installing the TOE in a manner that maintains IT security includes correctly configuring the TOE. As part of installing the TOE, the TOE will be properly configured. This objective provides for secure installation and configuration of the TOE.
- ON.Operations: The authorized administrator will ensure the proper procedures and guidelines in the guidance documentation are being followed and carry out during installation, configuration, managing, and operating of the TOE in a secure manner. The procedures will provide guidance to the authorized administrator on how to securely operate the TOE. This objective provides for operation procedures to be in place.

ON.Person: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system. This objective provides for competent personnel to correctly configure and operate the TOE. A.Manage: It is assumed that one or more authorized administrators are assigned who are competent to manage the TOE and the security of the information it contains, and who can be trusted not to deliberately abuse their privileges so as to undermine security. A.Manage is covered by:

- ON.Person: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system. This objective provides for competent personnel to administer the TOE.

A.No_Untrusted: It is assumed that there will be no untrusted users and no untrusted software on the Siebel eBusiness Platform Server host. A.No_Untrusted is covered by:

- ON.No_Untrusted: The authorized administrator will ensure that there are no untrusted users and no untrusted software on the Siebel eBusiness Platform Server host. This objective corresponds directly to the assumption.

A.Physical: The TOE components critical to the security policy enforcement will be protected from unauthorized physical modification. A.Physical is covered by:

- ON.Physical: Those responsible for the TOE will ensure that those parts of the TOE critical to the security policy are protected from any physical attack. This objective provides for the physical protection of the TOE hardware and software.

A.Time: It is assumed that the underlying the operating system provides reliable time stamps. A.Time is covered by:

- OE.Time: The underlying operating system will provide reliable time stamps. This objective provides for reliable time stamps.

A.Users: It is assumed that users will protect their authentication data. A.Users is covered by:

- ON.Protect_Auth: The users will ensure that their authentication data is held securely and not disclosed to unauthorized persons. This objective provides for users protecting their authentication data.

A.Users_Pass: It is assumed that there is the capability to hash and store user passwords. A.User_Pass is covered by:

- OE.Stored_Hash_Pass: The IT environment will hash the stored passwords. This objective provides for stored user passwords being hashed.

8.2 Security Requirements Rationale

8.2.1 Functional Requirements

Table 8-4 shows that all of the security objectives of the TOE are satisfied.

Table 8-4 All Objectives Met by Functional Components

Item	Objective	No.	Security Functional Requirement
1	O.Access	4	FAU_SAR.2 Restricted audit review
		7	FDP_ACC.2 Complete access control
		8	FDP_ACF.1 Security attribute based access control
		11	FIA_USB.1 User-subject binding
		12	FMT_MOF.1 Management of security functions behaviour
		13	FMT_MSA.1* Management of security attributes
		14	FMT_MSA.3 Static attribute initialisation
		15	FMT_MTD.1 Management of TSF data
2	O.Admin	3	FAU_SAR.1 Audit review
		5	FAU_SAR.3 Selectable audit review
		6	FAU_SEL.1 Selective audit
		12	FMT_MOF.1 Management of security functions behaviour
		13	FMT_MSA.1* Management of security attributes
		14	FMT_MSA.3 Static attribute initialisation
		15	FMT_MTD.1 Management of TSF data
		16	FMT_SMF.1 Specification of management functions
3	O.Attributes	9	FIA_ATD.1 User attribute definition
4	O.Audit	1	FAU_GEN.1 Audit data generation
		2	FAU_GEN.2 User identity association
		6	FAU_SEL.1 Selective audit
5	O.NonBypass	18	FPT_RVM_EXP.1-1 Non-bypassability of the TSP
6	O.Partial_Domain_Sep	19	FPT_SEP_EXP.1-1 TSF domain separation
7	O.Protect_Auth	10	FIA_UAU.7 Protected authentication feedback
8	O. Responsibilities	17	FMT_SMR.1 Security roles

O.Access: The TOE will provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the Siebel eBusiness Platform Access Control SFP. O.Access is addressed by:

- FAU_SAR.2 Restricted audit review, which requires that access to audit data be restricted to authorized users.
- FDP_ACC.2 Complete access control, which requires that the TSF enforce access controls on all operations between any subject in the TSC and any object within the TSC.
- FDP_ACF.1 Security attribute based access control, which requires the TSF enforce access controls based on specified security attributes.
- FIA_USB.1 User-subject binding, which requires that the TSF associates all user security attributes with subjects acting on behalf of the user.
- FMT_MOF.1 Management of Security Functions Behaviour, which restricts the ability to disable, enable, and modify functions to authorized users.
- FMT_MSA.1* Management of security attributes, which requires only authorized users can query, modify, and delete specified security attributes.
- FMT_MSA.3 Static attribute initialization, which requires the TSF enforce access control for specified default values of security attributes.
- FMT_MTD.1 Management of TSF data, which specifies the management of TSF Data according to assigned responsibilities.

O.Admin: The TOE will provide the functionality to enable an authorized administrator to effectively manage the TOE and its security functions. O.Admin is addressed by:

- FAU_SAR.1 Audit review, which requires that the authorized administrator be able to read audit records.
- FAU_SAR.3 Selectable Audit Review, which requires that the TSF will provide the ability to search, sort, and order audit data.
- FAU_SEL.1 Selective audit, which requires the TOE to provide authorized users with the ability to include or exclude auditable events from the set of audited events.
- FMT_MOF.1 Management of security functions behaviour, which requires that the authorized administrator be able to manage the behaviour of the audit function.
- FMT_MSA.1* Management of security attributes, which requires only authorized users can query, modify, and delete specified security attributes.
- FMT_MSA.3 Static attribute initialization, which requires the TSF enforce access control for specified default values of security attributes.
- FMT_MTD.1 Management of TSF Data, which specifies the management of TSF Data according to assigned responsibilities.
- FMT_SMF.1 Specification of management functions, which requires the TSF be capable of performing the specified security management functions.

O.Attributes: The TOE will be able to maintain user security attributes. O.Attributes is addressed by:

- FIA_ATD.1 User attribute definition, which requires that the TSF maintain security attributes of users.

O.Audit: The TOE will provide the capability to detect and create records of security-relevant events associated with users. O.Audit is addressed by:

- FAU_GEN.1 Audit data generation, which requires the ability to audit specified events.
- FAU_GEN.2 User identity association, which requires the ability to associate an auditable event with a specific user.
- FAU_SEL.1 Selective audit, which requires the TOE to provide authorized users with the ability to include or exclude auditable events from the set of audited events.

O.NonBypass: The TOE will ensure the TOE's access control policy (Table 5-2) is invoked and succeeds before allowing another TOE function to proceed. O.NonBypass is addressed by:

- FPT_RVM_EXP.1-1 Non-bypassability of the TSP, which requires that TSP enforcement functions are invoked and succeed before a security-relevant function is allowed to proceed.

O.Partial_Domain_Sep: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. O.Partial_Domain_Sep is addressed by:

- FPT_SEP_EXP.1-1 TSF domain separation, which requires that the TSF maintain a security domain for its own execution that protects it from interference and tampering by untrusted users. The TSF will enforce separation between security domains of subjects in the TSC.

O.Protect_Auth: The TOE will provide protected authentication feedback during user login. O.Protect_Auth is addressed by:

- FIA_UAU.7 Protected authentication feedback, the TSF shall provide only a display of the typed in user name and asterisks for the password for password authentication.

O. Responsibilities: The TOE will support multiple administrative responsibilities (roles). O. Responsibilities is addressed by:

- FMT_SMR.1 Security roles, which requires that the TSF maintain multiple administrative roles (responsibilities).

8.2.2 Dependencies

Table 8-5 shows the dependencies between the functional requirements. All dependencies are satisfied. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference. If the TOE dependency is met by an SFR in the IT environment an "E" will be next to the reference number.

Table 8-5 TOE Dependencies Satisfied

No.	Component	Component Name	Dependencies	Reference
1.	FAU_GEN.1	Audit data generation	FPT_STM.1	28 E
2.	FAU_GEN.2	User identity association	FAU_GEN.1	1
			FIA_UID.1	24 E (H)
3.	FAU_SAR.1	Audit Review	FAU_GEN.1	1
4.	FAU_SAR.2	Restricted Audit Review	FAU_SAR.1	3
5.	FAU_SAR.3	Selectable Audit Review	FAU_SAR.1	3
6.	FAU_SEL.1	Selective audit	FAU_GEN.1	1
			FMT_MTD.1	15
7.	FDP_ACC.2	Complete access control	FDP_ACF.1	8
8.	FDP_ACF.1	Security attribute based access control	FDP_ACC.1	7 (H)
			FMT_MSA.3	14
9.	FIA_ATD.1	User attribute definition	None	None
10.	FIA_UAU.7	Protected authentication feedback	FIA_UAU.1	23 E (H)
11.	FIA_USB.1	User-subject binding	FIA_ATD.1	9
12.	FMT_MOF.1	Management of security functions behaviour	FMT_SMR.1	17
			FMT_SMF.1	16

No.	Component	Component Name	Dependencies	Reference
13.	FMT_MSA.1*	Management of security attributes	FDP_ACC.1	7 (H)
			FMT_SMR.1	17
			FMT_SMF.1	16
14.	FMT_MSA.3	Static attribute initialization	FMT_MSA.1	13
			FMT_SMR.1	17
15.	FMT_MTD.1	Management of TSF data	FMT_SMR.1	17
			FMT_SMF.1	16
16.	FMT_SMF.1	Specification of Management Functions	None	None
17.	FMT_SMR.1	Security roles	FIA_UID.1	24 E (H)
18.	FPT_RVM_EXP.1-1	Non-bypassability of the TSP	None	None
19.	FPT_SEP_EXP.1-1	TSF domain separation	None	None

Table 8-6 IT Environment Dependencies are Satisfied

No.	Component	Component Name	Dependencies	Reference
20.	FCS_CKM.1*	Cryptographic key generation	FCS_COP.1	22 E
			FCS_CKM.4	21 E
			FMT_MSA.2	25 E
21.	FCS_CKM.4	Cryptographic key destruction	FCS_CKM.1	20 E
			FMT_MSA.2	25 E
22.	FCS_COP.1*	Cryptographic operation	FCS_CKM.1	20 E
			FCS_CKM.4	21 E
			FMT_MSA.2	25 E
23.	FIA_UAU.2	User authentication before any action	FIA_UID.1	24 E (H)
24.	FIA_UID.2	User identification before any action	None	None
25.	FMT_MSA.2	Secure security attributes	ADV_SPM.1	See section 8.2.3
			FDP_ACC.1	7 (H)
			FMT_MSA.1	13
			FMT_SMR.1	17
26.	FPT_RVM_EXP.1-2	Non-bypassability of the TSP	None	None
27.	FPT_SEP_EXP.1-2	TSF domain separation: Operating System	None	None
28.	FPT_STM.1	Reliable time stamps	None	None
29.	FPT_ITC.1	Inter-TSF confidentiality during transmission	None	None

8.2.3 Rationale why dependencies are not met

For FMT_MSA.2, ADV_SPM.1 is not included because ADV_SPM.1 requires the TOE developer to provide an informal TOE security policy (TSP) model. The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled. It is the objective of the ADV_SPM family to provide additional assurance that the security functions in the functional specification

enforce the policies in the TSP. This is accomplished via the development of a security policy model that is based on a subset of the policies of the TSP, and establishing a correspondence between the functional specification, the security policy model, and these policies of the TSP. Since the cryptographic functions are provided by the environment and not by the TOE, the functional specification will not include the cryptographic functions. As a result, there is no way to map the functional specification to the security policy model.

8.2.4 Strength of Function

A strength of function level of SOF-Basic counters an attack level of low. The environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product. A user password is required to be used when accessing the Administrator and User Interface. Since FIA_UAU.2 and FIA_UID.2 are in the IT environment, the login is out of scope for the TOE. Therefore, there is not a specific SOF claim mapped to an SFR. SOF analysis is described in Section 6.

8.2.5 Assurance Requirements

Evaluation Assurance Level EAL2 was chosen to provide a basic level of assurance due to the low level threat of malicious attacks.

8.2.6 Rationale that IT Security Requirements are Internally Consistent

The IT Security Requirements are internally consistent. There are no requirements that conflict with one another. When different IT security requirements apply to the same event, operation, or data there is no conflict between the security requirements. The requirements mutually support each other to apply to the event, operation, or data.

For auditing, each of the SFRs builds on the others. For example, FAU_GEN.1 details the auditable events generated by the TSF. FAU_GEN.2 provides for the TSF to associate each auditable event with the identity of the user that caused the event. FAU_SAR.1 states that the TSF shall provide the Siebel Administrator with the capability to read all audit information from the audit records. FAU_SAR.2 builds on FAU_SAR.1 by stating the TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. FAU_SAR.3 gives the authorized administrator the ability to perform searches and sorting of the audit event data. FAU_SEL.1 allows the authorized administrator to include or exclude auditable events from the set of audited events. Audit records are generated for many events where other requirements are coming to bear, such as login, policy check failures, and management functions.

Together FDP_ACC.2 and FDP_ACF.1 provide User Data Protection. FDP_ACC.2 defines the Siebel eBusiness Platform Access Control SFP. FDP_ACF.1 specifies that the TSF enforce access based upon security attributes and named groups of attributes (FIA_ATD.1). FIA_USB.1 associates the user security attributes defined in FIA_ATD.1 with the subjects acting on behalf of the user. The subjects with responsibilities (roles) of the following listed in Table 5-2 (FDP_ACC.2) are also defined in FMT_SMR.1.

Login processing brings in elements of many requirements, but all in a complementary way. FIA_UAU.7 requires that feedback from authentication input be obscured. The IT environment, on initiation from the TOE, enforces the identification (FIA_UID.2) and authentication (FIA_UAU.2) before allowing any other operations, via the use of an LDAP Server.

The management requirements (FMT_) are related to many of the mechanisms involved with other requirements. FMT_MOF.1 provides for the management of the audit functions (FAU_GEN.1).

FMT_MSA.1 enforces the Siebel eBusiness Platform Access Control SFP (FDP_ACC.2). FMT_MSA.3 enforces the Siebel eBusiness Platform Access Control SFP to provide restrictive default values for security attributes. FMT_MTD.1 specifies the management of TSF Data according to assigned responsibilities. FMT_SMF.1 specifies the security management functions of the TSF. In many cases, the other mechanisms will enforce the settings made through management functions. Installation mechanisms (see ADO_IGS.1) rely on management functions. The administrator guidance (see AGD_ADM) documents the management functions.

FPT_RVM_EXP.1-1 makes certain the Siebel eBusiness Platform Access Control SFP (FDP_ACC.2) is invoked and succeeds before any other functions within the TOE's Scope of Control are allowed to proceed. FPT_SEP_EXP.1-1 relies partly on FDP_ACC.2 to provide partial protection against unauthorised subjects from gaining access to the TOE's administrative interface.

8.2.7 Explicitly Stated Requirements Rationale

FPT_RVM_EXP.1* and FPT_SEP_EXP.1* had to be explicitly stated because they all provide partial TOE self-protection while relying on the OS and Hardware platforms to provide the full protection. According to CCIMB RI#19, which states the following: "Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use (i.e. applying the operation of iteration) of the same Part 2 components to cover each aspect is possible. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE. "

8.2.8 Requirements for the IT Environment

Table 8-7 shows that all of the security objectives for the IT environment are satisfied.

Table 8-7 All Objectives for the IT Environment Met by Requirements

Item	Objective	Requirement for the IT Environment	Component Title
9	OE.Partial_Domain_Sep	FMT_MSA.2	Secure security attributes
		FPT_SEP_EXP.1-2	TSF domain separation
10	OE.Protect_Comm	FCS_CKM.1-1	Cryptographic key generation
		FCS_CKM.4	Cryptographic key destruction
		FCS_COP.1-1	Cryptographic operation
		FPT_ITC.1	Inter-TSF confidentiality during transmission
11	OE.Stored_Hash_Pass	FCS_COP.1-2 FCS_CKM.1-2	Cryptographic operation: Hashing Function
12	OE.Time	FPT_STM.1	Reliable time stamps
13	OE.NonBypass	FPT_RVM_EXP.1-2	Non-bypassability of the TSP
14	OE.ID_Auth	FIA_UAU.2	User authentication before any action

Item	Objective	Requirement for the IT Environment	Component Title
		FIA_UID.2	User identification before any action

OE.Partial_Domain_Sep: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. OE.Partial_Domain_Sep is addressed by:

- FMT_MSA.2 Secure security attributes, which requires the IT environment to ensure only secure values are accepted for security attributes. This relates to the cryptographic functions and requires that only secure algorithms and key sizes can be configured.
- FPT_SEP_EXP.1-2 TSF domain separation, which requires the Operating System to maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through the Operating System's Interface. The IT environment will enforce separation between security domains of subjects in the Operating System's Scope of Control.

OE.Protect_Comm: The IT environment will protect communications between its components. OE.Protect_Comm is addressed by:

- FCS_CKM.1-1, Cryptographic key generation, which requires the IT environment generate cryptographic keys in accordance with a specified cryptographic key generation algorithm and specified cryptographic key sizes that meet a specified standard.
- FCS_CKM.4 Cryptographic key destruction, which requires the IT environment shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method.
- FCS_COP.1-1, Cryptographic operation, which requires that the IT environment perform cryptographic operations in accordance with a specified cryptographic algorithm and cryptographic key sizes that meet a specified standard.
- FPT_ITC.1, Inter-TSF confidentiality during transmission, which requires the IT environment to protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission.

OE.Stored_Hash_Pass The IT environment will hash the stored passwords. OE.Stored_Hash_Pass is addressed by:

- FCS_COP.1-2 Cryptographic operation: Hashing Function, which requires the IT environment to provide hashing functions to hash the user passwords that are stored in the database or directory.
- FCS_CKM.1-2, Cryptographic key generation, which requires the IT environment generate cryptographic keys in accordance with a specified cryptographic key generation algorithm and specified cryptographic key sizes that meet a specified standard.

OE.Time The underlying operating system will provide reliable time stamps. OE.Time is addressed by:

- FPT_STM.1 Reliable time stamps, which requires that time stamps be provided by the IT environment.

OE.NonBypass: The IT environment will ensure that its security functions cannot be bypassed. OE.NonBypass is addressed by:

- FPT_RVM_EXP.1-2: Non-bypassability of the TSP, which requires that the Operating Systems's Security Policy is invoked and succeeds before a security-relevant function is allowed to proceed.

OE.ID_Auth: The IT environment will be able to identify and authenticate users prior to allowing access to authorized TOE functions and data. OE.ID_Auth is addressed by:

- FIA_UAU.2 User authentication before any action, which requires the IT environment to successfully authenticate each user before allowing access to the TOE.

- FIA_UID.2 User identification before any action, which requires the IT environment successfully identify each user before allowing access to the TOE.

Table 8-8 has been included as a consistency check to show that the security functional requirements for the TOE map to the security objectives of the TOE.

Table 8-8 Mapping of TOE Functional Requirements to IT Security Objectives

No.	Requirement	Component Name	Objective
1.	FAU_GEN.1	Audit data generation	O.Audit
2.	FAU_GEN.2	User identity association	O.Audit
3.	FAU_SAR.1	Audit Review	O.Admin
4.	FAU_SAR.2	Restricted Audit Review	O.Access
5.	FAU_SAR.3	Selectable Audit Review	O.Admin
6.	FAU_SEL.1	Selective audit	O.Admin O.Audit
7.	FDP_ACC.2	Complete access control	O.Access
8.	FDP_ACF.1	Security attribute based access control	O.Access
9.	FIA_ATD.1	User attribute definition	O.Attributes
10.	FIA_UAU.7	Protected authentication feedback	O.Protect_Auth
11.	FIA_USB.1	User-subject binding	O.Access
12.	FMT_MOF.1	Management of Security Functions Behaviour	O.Access O.Admin
13.	FMT_MSA.1*	Management of security attributes	O.Access O.Admin
14.	FMT_MSA.3	Static attribute initialisation	O.Access O.Admin
15.	FMT_MTD.1	Management of TSF data	O.Access O.Admin
16.	FMT_SMF.1	Specification of management functions	O.Admin
17.	FMT_SMR.1	Security roles	O.Responsibilities
18.	FPT_RVM_EXP.1-1	Non-bypassability of the TSP	O.NonBypass
19.	FPT_SEP_EXP.1-1	TSF domain separation	O.Partial_Domain_Sep

Table 8-9 has been included as a consistency check to show that the security functional requirements for the IT environment map to the security objectives of the environment.

Table 8-9 SFRs in the environment

No.	Requirement	Component Name	Objective
21	FCS_CKM.1-1	Cryptographic key generation	OE.Protect_Comm
22	FCS_CKM.1-2	Cryptographic key generation	OE.Stored_Hash_Pass
23	FCS_CKM.4	Cryptographic key destruction	OE.Protect_Comm
24	FCS_COP.1-1	Cryptographic operation	OE.Protect_Comm
25	FCS_COP.1-2	Cryptographic operation	OE.Stored_Hash_Pass

No.	Requirement	Component Name	Objective
26	FIA_UAU.2	User authentication before any action	OE.ID_Auth
27	FIA_UID.2	User identification before any action	OE.ID_Auth
28	FMT_MSA.2	Secure security attributes	OE.Partial_Domain_Sep
29	FPT_RVM_EXP.1-2	Non-bypassability of the TSP	OE.NonBypass
30	FPT_SEP_EXP.1-2	Domain separation	OE.Partial_Domain_Sep
31	FPT_STM.1	Reliable time stamps	OE.Time
32	FPT_ITC.1	Inter-TSF confidentiality during transmission	OE.ProtectComm

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

Table 8-10 shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 8-10 Mapping of Functional Requirements to TOE Summary Specification

No	Functional Component	Functional Requirement	Requirement is met by:	
			Security Function Ref. No	Rationale
1	FAU_GEN.1	Audit data generation	AI-SA-1	Specifies the types of events to be audited.
			AI-SA-2	Specifies the information to be recorded in an audit record.
2	FAU_GEN.2	User identity association	AI-SA-3	Each auditable event is associated with the identity of the user that caused the event.
3	FAU_SAR.1	Audit review	AI-SA-4	Specifies who has the capability to read information from the audit records.
			AI-SA-5	
4	FAU_SAR.2	Restricted audit review	AI-SA-6	Specifies that only specific users have read access to the audit records.
5	FAU_SAR.3	Selectable audit review	AI-SA-7	Specifies Siebel eBusiness Platform provides the ability to perform searches and sorting of the audit data based on various criteria.
6	FAU_SEL.1	Selective audit	AI-SA-8	Specifies Siebel eBusiness Platform is able to include or exclude auditable events from the set of audited events based on specific attributes.
7	FDP_ACC.2	Complete access control	AI-MUA-1	Specifies the Siebel eBusiness Platform Access Control SFP.
8	FDP_ACF.1	Security attribute based access control	AI-MUA-1	Specifies the subjects and objects controlled under the Siebel eBusiness Platform Access Control SFP.

9	FIA_ATD.1	User attribute definition	AI-MUA-2	Specifies the security attributes maintained for each user.
10	FIA_UAU.7	Protected authentication feedback	AI-UL-1	Specifies the Siebel eBusiness Platform Administrative Interface displays only the typed in user name and asterisks for the password during password authentication.
11	FIA_USB.1	User-subject binding	AI-MUA-3	Specifies that the Siebel eBusiness Platform shall associate all user security attributes with subjects acting on behalf of that user.
12	FMT_MOF.1	Management of security functions behaviour	AI-SM-1	Specifies that the Siebel eBusiness Platform restricts the ability to determine the behaviour of, disable, enable, and modify the behaviour of the functions related to the selection of which auditable events (see FAU_SEL.1.1) and the audit function (see FAU_GEN.1.1) to the Siebel Administrator.
13 a	FMT_MSA.1-1	Management of security attributes	AI-SM-2	Specifies that the Siebel eBusiness Platform restricts the ability to query, modify, delete, create, and rename the user identity attributes to the Siebel Administrator.
13 b	FMT_MSA.1-2	Management of security attributes	AI-SM-3	Specifies that Siebel eBusiness Platform restricts the ability to query, modify, delete, or create the responsibility and access groups attributes to the Siebel Administrator.
13 c	FMT_MSA.1-3	Management of security attributes	AI-SM-4	Specifies that the Siebel eBusiness Platform restricts the ability to change_default, query, modify, or create the organization attribute to the Siebel Administrator.
13 d	FMT_MSA.1-4	Management of security attributes	AI-SM-5	Specifies that the Siebel eBusiness Platform restricts the ability to query, modify, or create the divisions attribute to the Siebel Administrator.
13 e	FMT_MSA.1-5	Management of security attributes	AI-SM-6	Specifies that the Siebel eBusiness Platform restricts the ability to query, modify, rename, or create the positions attribute to the Siebel Administrator.
14	FMT_MSA.3	Static attribute initialisation	AI-SM-7	Specifies that the Siebel eBusiness Platform provides restrictive default values for security attributes and the Siebel Administrator can specify alternative initial values.

15	FMT_MTD.1	Management of TSF data	AI-SM-8	Specifies that the Siebel eBusiness Platform restricts the ability to access data.
16	FMT_SMF.1	Specification of management functions	AI-SM-9	Specifies the security management functions provided by the Siebel eBusiness Platform.
17	FMT_SMR.1	Security roles	AI-SM-10	Specifies the responsibilities (roles) maintained.
18	FPT_RVM_EXP.1-1	Non-bypassability of the TSP	AI-MUA-4	Specifies the Siebel eBusiness Platform ensures that the Table 5-2 Siebel eBusiness Platform Access Control SFP is invoked and succeeds before each function is allowed to proceed.
19	FPT_SEP_EXP.1-1	Domain separation	AI-MUA-5	Specifies the Siebel eBusiness Platform maintains a security domain for its own execution and enforces separation between the security domains of users. The Siebel eBusiness Platform Access Control SFP is used to protect TSF data from tampering.

8.3.2 Assurance Measures

The assurance measures rationale shows how all assurance requirements are satisfied. The rationale is provided in Table 8-11.

Table 8-11 Assurance Measures Rationale

Component	Evidence Requirements	How Satisfied	Rationale
ACM_CAP.2	CM Documentation • CM Proof • Configuration Item List	• Siebel CM Plan V1.0 • Siebel Version Control and Number Scheme • clearcase_snapshot_views • developers_guide_nt • developers_quick_ref_guide • Siebel_7.x_SS_BranchSS_ BuildProcedures	• CM Proof - Show proof that CM system is being used for development. • Configuration Item List(s) - TOE version including Build Number - is comprised of a list of design documents with version numbers - is comprised of test documents with version numbers - user and administrator documentation with version numbers
ADO_DEL.1	Delivery Procedures	- Shipping process doc v3.doc - Shipping Process.pdf - Building Product Kits.doc - rmr_mr_process_qe_release_perspective.doc	Provides a description of all procedures that are necessary to maintain security when distributing TOE software to the user's site. - Applicable across all phases of delivery from packaging, storage, distribution
ADO_IGS.1	Installation, generation, and start-up procedures	- AppsAdmin_7.8.pdf - SiebInstWIN_7.8.pdf	Provides detailed instructions on how to install Siebel eBusiness Platform.
ADV_FSP.1	Functional Specification	Siebel eBusiness Platform FSP v1.3.doc	Provides rationale that TSF is fully represented
		Applications Administration Guide v7.8,	Describes the TSF interfaces and TOE functionality
		Security Guide for Siebel Business Applications v7.8	Describes TOE functionality

Component	Evidence Requirements	How Satisfied	Rationale
ADV_HLD.1	High-Level Design	ADV_HLD v9.doc	Describes the TOE subsystems and their associated security functionality
ADV_RCR.1	Representation Correspondence	ADV_RCR Specification v1.1.doc	Provides the following two dimensional mappings: 1. TSS and functional specification; 2. functional specification and high-level design.
AGD_ADM.1	Administrator Guidance	Applications Administration Guide v7.8	Describes how to administer the TOE securely.
		Security Guide for Siebel Business Applications v7.8	Describes how to administer the TOE securely.
AGD_USR.1	User Guidance	Applications Administration Guide v7.8	Describes the secure use of the TOE.
		Security Guide for Siebel Business Applications v7.8	Describes how to use the TOE securely.
ATE_COV.1	Test Coverage Analysis	Siebel Test Coverage Analysis V1.0	Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_FUN.1	Test Documentation	Siebel Test Plan and Report v2.0 with Test Cases.	Test documentation includes test plans and procedures and expected and actual results.
ATE_IND.2	TOE for Testing	TOE for Testing	The TOE will be provided for testing.
AVA_SOF.1	SOF Analysis	Not required. This TOE does not have mechanisms based on permutations.	Provides a rationale that each mechanism identified in the ST as having an SOF meets or exceeds the minimum strength level specified there.
AVA_VLA.1	Vulnerability Analysis	Siebel Vulnerability Analysis V 1.0	Provide an analysis of the TOE deliverables for obvious ways in which a user can violate the TSP, including the disposition of obvious vulnerabilities.

8.4 PP Claims Rationale

Not applicable. There are no PP claims.

9 Appendix

9.1 Acronyms

Table 9-1 Acronyms

Acronym	Description
ACM	Configuration Management
ADO	Delivery and Operation
ADV	Development
AES	Advanced Encryption Standard, FIPS PUB 197.
AGD	Guidance Documents
ALC	Life cycle support
ATE	Tests
AVA	Vulnerability assessment
CC	Common Criteria [for IT Security Evaluation]
CCIMB	Common Criteria Interpretations Management Board
DBMS	Database Management System
EAL	Evaluation Assurance Level
FAU	Security Audit
FCO	Communication
FCS	Cryptographic Support
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FPT	Protection of the TSF
FTA	TOE Access
FTP	Trusted Channels/Path
GUI	Graphical User Interface
ID	Identifier
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
OS	Operating System
PP	Protection Profile
SAS	Siebel Application Server
SHA-1	Secure Hash Standard (SHS), FIPS PUB 180-2
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation

Acronym	Description
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UI	User Interface

9.2 References

Table 9-2 References

File name	Document Title
CCITSE	*Common Criteria for Information Technology Security Evaluation*, CCIMB-2004-01-002, Version 2.2, January 2004.
AppsAdmin.pdf	Applications Administration Guide v7.8, RevA
Doc_eBusiness_Platform.pdf	Siebel 7 eBusiness Platform
Security-Hardening Document v12.pdf	Siebel eBusiness Securing Siebel eBusiness Applications (Hardening Guide)
Siebel Security Guide 7.8.pdf	Siebel eBusiness Security Guide for Siebel Business Applications v7.8
WP_Security.pdf	Security for Siebel eBusiness Applications (White Paper)
SystAdm.pdf	Siebel System Administration Guide V7.8
7.8.2_MR_Guide.pdf	Maintenance Release Guide V7.8.2
7_8_Reqs_Platform_RevE.pdf	Siebel System Requirements and Supported Platforms Business Applications Version 7.8, Rev. E
SiebInstWIN.pdf	Siebel Installation Guide for Microsoft Windows: Servers, Mobile Web Clients, Tools Version 7.8, Rev. A