SAIC TeraText DBS 4.3.13 Security Target

Version 1.02

5/22/08

Prepared for:

Science Applications International Corporation

1997 Annapolis Exchange Parkway, Suite 200
Annapolis, Maryland 21401

Prepared By:

Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is SAIC TeraText Dastabase System (DBS) 4.3.13 provided by Science Applications International Corporation (SAIC).

The Security Target contains the following additional sections:

- Section 2 – Target of Evaluation (TOE) Description
  This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Section 3 – TOE Security Environment
  This section details the expectations of the environment, the threats that are countered by TeraText DBS 4.3.13 and IT environment, and the organizational policy that TeraText TOE 4.3.13 must fulfill.
- Section 4 – TOE Security Objectives
  This section details the security objectives of the TeraText DBS 4.3.13 and IT environment.
- Section 5 – IT Security Requirements
  The section presents the security functional requirements (SFR) for TeraText DBS 4.3.13 and IT Environment that supports the TOE, and details the assurance requirements for EAL2.
- Section 6 – TOE Summary Specification
  The section describes the security functions represented in the TeraText DBS 4.3.13 that satisfy the security requirements.
- Section 7 – Protection Profile Claims
  This section presents any protection profile claims.
- Section 8 – Rationale
  This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – SAIC TeraText DBS 4.3.13 Security Target

ST Version – Version 1.02

ST Date – 05/22/2008

TOE Identification – SAIC TeraText DBS 4.3.13

TOE Developer – SAIC

Evaluation Sponsor – SAIC

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.2, Revision 256, January 2004.

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.2, Revision 256, January 2004.
  - Part 2 Conformant

- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.2, Revision 256, January 2004.
  - Part 3 Conformant
  - Evaluation Assurance Level: EAL 2
  - Strength of Function Claim: SOF-basic

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.
- Explicitly stated SFRs (i.e., those not found in Part 2 of the CC) are identified with "_EX". Example: Audit data generation (FAU_GEN_EX.1)
- The TOE's official name is SAIC TeraText DBS 4.3.13. Throughout this ST and the evaluation evidence, the TOE may be generically referred to as TeraText DBS or just TeraText.

2. TOE Description

The Target of Evaluation (TOE) is SAIC TeraText DBS 4.3.13 for Solaris, a database server application.

There are no differences between the product and the TOE. The TOE is a database server application that is optimized for managing records containing text. The TOE manages text documents in a variety of formats and encodings including HTML, SGML, XML, RTF, MARC, spreadsheets, word processor documents, plain text, Unicode, and images. It is not a relational database system.

The remainder of this section summarizes the TOE architecture.

2.1 TOE Overview

The TOE is a database server application that is for managing records containing text. The TOE is not a relational database system.

The TOE manages text documents in a variety of formats and encodings including HTML, SGML, XML, RTF, MARC, spreadsheets, word processor documents, plain text, Unicode, and images. It also supports storing images and other non-text formats. For textual data, the TOE provides full text indexing and searching capabilities such as word, field and phrase based querying, fuzzy matching, word stemming, Boolean operators, word distance (proximity) operators, ranking, results sorting, and term highlighting.

The TOE is based on the ANSI Z39.50 protocol, an international standard for distributed search and retrieval. This enables the TOE to scale across multiple servers in order to support large text collections. In this architecture, text is stored in “databases” and databases reside in “content servers”. Databases are somewhat analogous to “tables” in a relational database system. However, one key difference is that Z39.50 enables databases with different physical structures to be accessed as if they have a uniform structure. This is not the case with relational database tables. The TOE also uses a query language that is quite distinct from the Structured Query Language (SQL) used by relational databases.

2.2 TOE Architecture

The TOE manages text documents stored in databases. Before documents can be stored in a database, a database schema must first be defined that specifies the physical structure of the database, the logical elements (fields) to search on, text indexing parameters, and row and column security constraints. Indexes can be specified on an element-by-element basis, for example, the title of a document could be indexed as a complete phrase and the rest of the document as individual words, with or without word proximity querying enabled.

Text documents can be stored in TOE databases as a record in the database (with optional compression), and record contents (i.e. the document) can then be indexed for searching. The TOE validates records as they are entered to ensure that data definitions and data content are in agreement.

Text documents can be searched using the TOE by end users after establishing an authenticated Z39.50 network protocol connection using either TOE interfaces, which include for example programming interfaces that abstract Z39.50 protocol commands. After a user has connected to the TOE, after the user has successfully authenticated to the TOE, a Z39.50 session is established for the user by TOE interfaces that abstract Z39.50 protocol commands. Z39.50 user sessions allow TOE interfaces (on behalf of calling users) to access and search documents using Z39.50 protocol commands.

When a user submits a query to the TOE, the query contains search terms (e.g., terms that the user has identified to be matched against access points in the database) and attributes of those search terms (e.g., specifying the terms as an "author" or "title," specifying if the terms are to be "truncated," etc.). Queries can include different attribute types. For example, if a user wants to search for an author's name, a "use" attribute specifies the search term as "author." If the user wants to search for all books published after a certain date, a "use" attribute specifies the search term is a "date of publication" and a "relation" attribute specifies that the user wants all dates of publication "greater than" a particular date. Z39.50 protocol defines these attribute types and their values in registered attribute sets.

After a user submits a query to the TOE, the TOE creates a result set consisting of those records that match the criteria of the query. Users can request that the TOE return those records from a result set, or they can issue additional searches that further qualify a result set or use result sets as arguments in subsequent searches. When the user wants to access records listed in the result set, Z39.50 protocol commands can be used to specify which data elements (i.e., element sets) from the database record to return. It also gives choices about the format for transferring the record (i.e., a record syntax) from the server to the client. Z39.50 protocol commands can be used to specify standardized element set names and record syntaxes to support this aspect of information retrieval.

The TOE can be described in terms of the following components, including the number of instances of each component that are supported in the evaluated configuration:

- TeraText Content Server application (one or more instances)
- TeraText Advanced Search Interface Server application (single instance)
- TeraText Command Line Interface Server application (single instance)
- TeraText APIs (one or more instances)
- TeraText Application Server application (single instance)
- TeraText Database Design Interface Server application (single instance)
- TeraText Security and Logging Server application (single instance)
- TeraText Boot Server application (single instance)
- TeraText Directory Server application (single instance)

The intended environment of the TOE can be described in terms of the following components:

- Operating system
- Web browser
- Java and .NET runtime environments

The TeraText Content Server application provides a database server application that can store and manage records containing text accessible using Z39.50 network protocol interfaces. The TeraText Content Server application also provides proprietary network protocol interfaces that are accessible using TeraText administrative console interfaces to manage server services.

The TeraText Advanced Search Interface Server application provides GUI interfaces that are accessible using a web browser via HTTP that calls the TeraText Command Line Interface Application subcomponent, and to generate Common Command Language (CCL) commands in order to access database services.

The TeraText Command Line Interface application provides Common Command Language (CCL) command-line interfaces that can be used to both establish Z39.50 network connections with the TeraText Content Server component, and to generate Z39.50 protocol commands in order to access database services.

The TeraText application programming interface (API) application provides Ace (a TeraText scripting language), Java, and .NET language programmatic interfaces that can be used to both establish Z39.50 network connections with the TeraText Content Server component, and to generate Z39.50 protocol commands in order to access database services.

The TeraText Application Server application provides a runtime environment (an interpreter) for Ace scripts.

The TeraText Database Design Interface Server application provides graphical user interface (GUI) administrative console interfaces that are accessible using a web browser via HTTP to create and manage databases using the TeraText Content Server component.

The TeraText Security and Logging Server application provides audit and username/password authentication mechanisms that are accessible via proprietary network protocol interfaces, as well as GUI administrative console interfaces that are accessible using a web browser via HTTP to manage users. Services provided by this subcomponent are relied on by other TeraText components and subcomponents.

The TeraText Boot Server application provides GUI administrative console interfaces that are accessible using a web browser via HTTP to start/stop TeraText component and subcomponent server applications.

The TeraText Directory Server application provides TeraText component and subcomponent server application host name and port information that are accessible via proprietary network protocol network protocol interfaces that is relied on by TeraText components and subcomponents to establish network connections with each other.

The operating system provides a runtime environment, as well as domain separation and non-bypassability, time stamp, audit review, and audit protection. The web browser provides runtime environment for TeraText components and subcomponents that provide GUI interfaces that are accessible using a web browser via HTTP. The Java and .NET runtime environments provide calling applications with ability to invoke TOE Java and .NET APIs.

2.2.1 Physical Boundaries

The components that make up the TOE are:

- TeraText Content Server application
- TeraText Advanced Search Interface Server application
- TeraText Command Line Interface Server application
- TeraText APIs
- TeraText Application Server application (combined with “TeraText APIs” component in figure below)
- TeraText Database Design Interface Server application
- TeraText Security and Logging Server application
- TeraText Boot Server application
- TeraText Directory Server application

The TOE depends on the following components that are **NOT** included in the TOE:

- Operating system – Sun Solaris 8
- Web browser – Internet Explorer 6.0 or more recent, Netscape 6.2 or more recent, Mozilla 1.2 or more recent, Opera 6.03 or more recent.
- Java 1.4.2 and .NET 1.1 runtime environments

The TOE in its intended environment is depicted in the figures below.

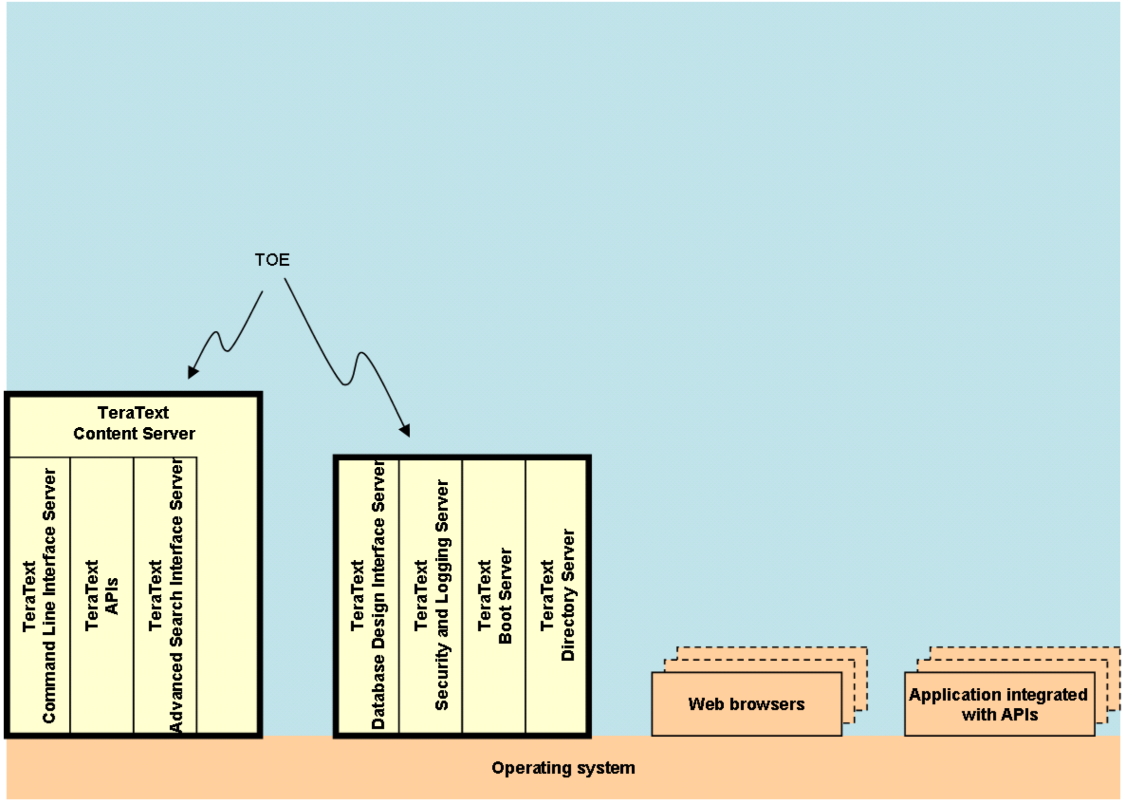
TOE
TeraText Content Server
TeraText Command Line Interface Server
TeraText APIs
TeraText Advanced Search Interface Server
TeraText Database Design Interface Server
TeraText Security and Logging Server
TeraText Boot Server
TeraText Directory Server
Web browsers
Application integrated with APIs
Operating system

Figure 1: TOE boundary

2.2.2 Logical Boundaries

The TSF provides the following security functions:

- Security audit
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access

2.2.2.1 Security audit

The TOE generates audit records which contain date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. Note that auditable events are associated with the identity of the user based on user identifier.

See the corresponding section in the TSS for more detailed information.

2.2.2.2 User data protection

The TOE can restrict access to Z39.50 databases, records, and schema elements to users and groups based on permissions.

See the corresponding section in the TSS for more detailed information.

2.2.2.3 Identification and authentication

The TOE ensures users are identified and authenticated prior to allowing them the ability to access the TOE's security functions. Users are identified with a user name and authenticated with a password. Users attributes include; user name, authentication data (password), and group membership.

See the corresponding section in the TSS for more detailed information.

2.2.2.4 Security management

The TOE provides administrator console interfaces that can be used by authorized administrators to perform all management functions, including: managing database subjects (including authentication data), database objects, and TOE session establishment IP addresses.

See the corresponding section in the TSS for more detailed information.

2.2.2.5 Protection of the TSF

The TOE can ensure that implicit and explicit policies that it enforces are not bypassed by controlling access to its interfaces, including separating client connections between users and the TOE, and between TOE components. The TOE also relies on its platform to operate correctly and to prevent unauthorized access to TOE data and stored executables

See the corresponding section in the TSS for more detailed information.

2.2.2.6 TOE access

The TeraText Content Server component of the TOE can restrict user sessions based on the IP address of the originating client connection (where client in this context is defined as TOE components and subcomponents that initiate Z39.50 connections with the TeraText Content Server).

See the corresponding section in the TSS for more detailed information.

2.3 TOE Documentation

SAIC offers a series of documents that describe the installation process for TeraText as well as guidance for subsequent use and administration of the applicable security features. Refer to Section 6 for information about these and other documentation associated with TeraText.

3. Security Environment

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed.

The statement of the TOE security environment defines the following:

- Threats that the TOE is designed to counter
- Assumptions made on the operational environment and the method of use intended for the TOE
- Organizational security policies which the TOE is designed to comply.

3.1 Organizational Policies

P.ACCOUNTABILITY The users of the TOE shall be held accountable for their actions within the TOE.

P.AUTHORIZATION The abilities of users of the TOE shall be limited in accordance with the TSP.

P.AUTHORIZED_USERS Access controls will ensure that only those users who have been authorized to access the protected information within the TOE will be able to do so.

P.I_AND_A All users must be identified and authenticated prior to accessing any controlled resources.

P.NEED_TO_KNOW The users of the TOE shall limit the access to information in protected resources to those authorized users who have a need to know that information.

P.ROLES The users of the TOE shall use an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

3.2 Threats

T.ADMIN_ERROR An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

T.AUDIT_COMPROMISE A process or user may cause audit data to be inappropriately accessed (viewed, modified or deleted), or prevent future records from being recorded, thus masking an attacker’s actions.

T.MASQUERADE An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.

T.SYSACC A malicious process or user may gain unauthorized access to the authorized administrator account, or that of other trusted personnel.

T.TSF_COMPROMISE An unauthorized user may gain access to the TOE and cause configuration data to be inappropriately accessed (viewed, modified or deleted).

T.UNAUTH_ACCESS A user may gain unauthorized access (view, modify, delete) to user data.

T.UNDETECTED_ACTIONS Unauthorized attempts to access TOE data or security functions may go undetected. .

T.UNIDENTIFIED_ACTIONS An authorized administrator may not be able to read audit records stored in the audit trail.

3.3 Assumptions

A.NO_EVIL Authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.

A.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g., compilers or user applications) available on TOE servers, other than those services necessary for the operation, administration and support of the TOE.

A.PHYSICAL It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.

A. ENVIRONMENT It is assumed that the IT environment provides support commensurate with the expectations of the TOE.

A.NETWORK It is assumed that the environment protects network communication media appropriately.

4. Security Objectives

4.1 Security Objectives for the TOE

O.ACCESS The TOE will ensure that users gain only authorized access to the TOE and to the resources that the TOE controls.

O.ADMIN_ROLE The TOE will provide authorized administrator roles to isolate administrative actions.

O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security relevant events associated with users.

O.DISCRETIONARY_ACCESS The TOE will control access to resources based upon the identity of users, group membership of users, and access control lists.

O.INTERNAL_TOE_DOMAINS The TSF will maintain internal domains for separation of data and queries belonging to concurrent users.

O.MANAGE The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

O.PROTECT The TOE will provide mechanisms to protect user data and resources.

O.TOE_PROTECTION The TOE will protect itself and its assets from external interference or tampering.

O.USER_AUTHENTICATION The TOE will verify the claimed identity of users.

O.USER_IDENTIFICATION The TOE will uniquely identify users.

4.2 Security Objectives for the IT Environment

OE.AUDIT_PROTECTION The IT environment will provide the capability to protect audit information.

OE.AUDIT_REVIEW The IT environment will provide the capability to view audit information, and alert the authorized administrator of identified potential security violations, using tools in the IT environment such as a text editor to review and search the audit trail file.

OE.TIME The IT environment will provide a time source that provides reliable time stamps.

OE.SELF_PROTECTION IT environment and its assets will be protected from external interference, tampering or unauthorized disclosure.

OE.TOE_PROTECTION The IT environment will provide protection to the TOE and its assets from external interference or tampering.

4.3 Security Objectives for the Non-IT Environment

OE.PERSON Authorized administrators of the TOE shall be properly trained in the configuration and usage of the TOE and will follow the guidance provided. These users are not careless, negligent, or hostile.

OE.CONFIG The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation and applicable security policies and procedures by appropriately trained and trusted administrator personnel.

OE.INSTALL The TOE will be delivered with the appropriate installation guidance to establish and maintain TOE security.

OE.NO_GENERAL_PURPOSE There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on TOE servers, other than those services necessary for the operation, administration and support of the TOE.

OE.PHYSICAL The environment in which the TOE operates is sufficient for secure operation. That the parts of the TOE critical to security policy are protected from physical attack and modification that might compromise the TOE security objectives.

OE.TRUST_IT Each IT entity the TOE relies on for security functions will be installed, configured, managed, maintained and provide the applicable security functions in a manner appropriate to the IT entity, and consistent with the security policy of the TOE and the relationship between them.

5. IT Security Requirements

This section defines the security functional requirements for the TOE as well as the security assurance requirements against which the TOE has been evaluated. All of the requirements have been copied from version 2.2 of the applicable Common Criteria documents.

5.1 TOE Security Functional Requirements

The following table describes the SFRs that are candidates to be satisfied by SAIC TeraText DBS 4.3.13

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit data generation
	FAU_GEN.2: User identity association
FDP: User data protection	FDP_ACC.1: Subset access control
	FDP_ACF.1: Security attribute based access control
FIA: Identification and authentication	FIA_ATD.1: User attribute definition
	FIA_UAU.2: User authentication before any action
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MSA.1: Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_MTD.1a: Management of TSF data
	FMT_MTD.1b: Management of TSF data
	FMT_MTD.1c: Management of TSF data
	FMT_REV.1a: Revocation
	FMT_REV.1b: Revocation
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_RVM.1a: Non-bypassability of the TSP
	FPT_SEP.1a: TSF domain separation
FTA: TOE access	FTA_TSE.1: TOE session establishment

Table 1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the **[*not specified*]** level of audit; and c) **[the following auditable events:**

- Successful requests to perform an operation on an object covered by the SFP
- Unsuccessful use of the authentication mechanism
- Unsuccessful use of the user identification mechanism, including the user identity provided

]. *(per International Interpretation #202)*

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, **[no additional information]**

5.1.1.2 User identity association (FAU_GEN.2)

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

5.1.2 User data protection (FDP)

5.1.2.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1 The TSF shall enforce the **[DAC SFP]** on **[all database subjects; the following database objects: databases, records, elements; and, all operations on the identified objects by database subjects]**.

5.1.2.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the **[DAC SFP]** to objects based on the following: **[database subject attributes: user identity, group membership; and, database object attributes: permissions]**. *(per International Interpretation #103)*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[**
a) if the user is granted the permission(s) for the requested access, the requested access is allowed;
b) if the user is a member of a group that is granted the permission(s) for the requested access, the requested access is allowed or
c) otherwise access is denied, unless access is explicitly authorized in accordance with the rules specified in FDP_ACF.1.3.].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[a) if the database subject is a member of the DBA group, the requested access is allowed; or b) if access is granted to all groups, the requested access is allowed.]**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **[following rules:**
a) if a user or a group of which a user is a member is denied access for the requested access, the requested access is denied.
b) If a requested access is both allowed and denied, denied takes priority and the requested access is denied.
c) if the operation in the request is not supported for the object type].

5.1.3 Identification and authentication (FIA)

5.1.3.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **[user identity, authentication data, group memberships]**.

5.1.3.2 User authentication before any action (FIA_UAU.2)

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

5.1.3.3 User identification before any action (FIA_UID.2)

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

5.1.4 Security management (FMT)

5.1.4.1 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the **[DAC SFP]** to restrict the ability to **[*modify*]** the security attributes **[of subjects and objects]** to **[authorized administrators]**.

5.1.4.2 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the **[DAC SFP]** to provide **[*restrictive*]** default values for security attributes that are used to enforce the SFP. *(per International Interpretations #201 and #202)*

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

5.1.4.3 Management of TSF data (FMT_MTD.1a)

FMT_MTD.1a.1 The TSF shall restrict the ability to **[*other operations:* set and reset, manage]** the **[subjects and authentication data]** to **[authorized administrators and the user associated with the authentication data]**.

5.1.4.4 Management of TSF data (FMT_MTD.1b)

FMT_MTD.1b.1 The TSF shall restrict the ability to **[*modify*]** the **[TOE session establishment IP addresses]** to **[authorized administrators]**.

5.1.4.5 Management of TSF data (FMT_MTD.1c)

FMT_MTD.1c.1 The TSF shall restrict the ability to **[*other operations:* manage]** the **[audit function]** to **[authorized administrators]**.

5.1.4.6 Revocation (FMT_REV.1a)

FMT_REV.1a.1 The TSF shall restrict the ability to revoke security attributes associated with the **[*subjects*]** within the TSC to **[authorized administrators]**. *(per International Interpretation #201)*

FMT_REV.1a.2 The TSF shall enforce the rules: **[the enforcement of subject attribute changes shall take effect upon the next login]**.

5.1.4.7 Revocation (FMT_REV.1b)

FMT_REV.1b.1 The TSF shall restrict the ability to revoke security attributes associated with the **[*objects*]** within the TSC to **[authorized administrators]**. *(per International Interpretation #201)*

FMT_REV.1b.2 The TSF shall enforce the rules: **[the enforcement of object attribute changes shall take effect before the next access attempt related to that object]**.

5.1.4.8 Specification of Management Functions (FMT_SMF.1)

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

a.) **management of database subjects and authentication data**

b.) **management of database objects**

c.) **management of TOE session establishment**

d.) **management of the audit function]**. *(per International Interpretation #65)*

5.1.4.9 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles **[authorized administrators and users]**.

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

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Non-bypassability of the TSP (FPT_RVM.1a)

FPT_RVM.1a.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.5.2 TSF domain separation (FPT_SEP.1a)

FPT_SEP.1a.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

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

5.1.6 TOE access (FTA)

5.1.6.1 TOE session establishment (FTA_TSE.1)

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on **[IP address]**.

5.2 IT Environment Security Functional Requirements

The following table describes the SFRs that are candidates to be satisfied by the IT environment of the TOE.

Requirement Class	Requirement Component
FAU: Security audit	FAU_SAR.1: Audit review
	FAU_STG.1: Protected audit trail storage
FPT: Protection of the TSF	FPT_RVM.1b: Non-bypassability of the TSP
	FPT_SEP.1b: TSF domain separation
	FPT_STM.1: Reliable time stamps

Table 2 IT Environment Security Functional Components

5.2.1 Security audit (FAU)

5.2.1.1 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The ~~TSF~~ **IT Environment** shall provide **[the authorized administrator]** with the capability to read **[all audit information]** from the audit records.

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

5.2.1.2 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The ~~TSF~~ **IT Environment** shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The ~~TSF~~ **IT Environment** shall be able to **[*prevent*]** unauthorised modifications to the audit records in the audit trail. *(per International Interpretations #141 and #202)*

5.2.2 Protection of the TSF (FPT)

5.2.2.1 Non-bypassability of the TSP (FPT_RVM.1b)

FPT_RVM.1b.1 The ~~TSF~~ **IT Environment** shall ensure that ~~TSP~~ **IT Environment** enforcement functions are invoked and succeed before each function within the ~~TSC~~ **IT Environment scope of control** is allowed to proceed.

5.2.2.2 TSF domain separation (FPT_SEP.1b)

FPT_SEP.1b.1 The ~~TSF~~ **IT Environment** shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1b.2 The ~~TSF~~ **IT Environment** shall enforce separation between the security domains of subjects in the ~~TSC~~ **IT Environment scope of control**.

5.2.2.3 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The ~~TSF~~ **IT Environment** shall be able to provide reliable time stamps for its own **and TOE** use.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.2: Configuration items
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.1: Descriptive high-level design
	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 3 EAL 2 Assurance Components

5.3.1 Configuration management (ACM)

5.3.1.1 Configuration items (ACM_CAP.2)

ACM_CAP.2.1d The developer shall provide a reference for the TOE.
ACM_CAP.2.2d The developer shall use a CM system.
ACM_CAP.2.3d The developer shall provide CM documentation.
ACM_CAP.2.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.2.2c The TOE shall be labelled with its reference.
ACM_CAP.2.3c The CM documentation shall include a configuration list.
ACM_CAP.2.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.2.6c The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.2.7c The CM system shall uniquely identify all configuration items.

ACM_CAP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2d The developer shall use the delivery procedures.

ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.

ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2c The functional specification shall be internally consistent.

ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4c The functional specification shall completely represent the TSF.

ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Descriptive high-level design (ADV_HLD.1)

ADV_HLD.1.1d The developer shall provide the high-level design of the TSF.

ADV_HLD.1.1c The presentation of the high-level design shall be informal.

ADV_HLD.1.2c The high-level design shall be internally consistent.

ADV_HLD.1.3c The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6c The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.
ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.
ADV_RCR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.
AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.
AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.
AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.
AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.
AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.
AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.
AGD_USR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Tests (ATE)

5.3.5.1 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1d The developer shall provide evidence of the test coverage.

ATE_COV.1.1c The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.

ATE_FUN.1.2d The developer shall provide test documentation.

ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.3 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.

ATE_IND.2.1c The TOE shall be suitable for testing.

ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.6 Vulnerability assessment (AVA)

5.3.6.1 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.6.2 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.

AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.

AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Security audit

The TOE generates audit records which contain date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. Note that auditable events are associated with the identity of the user based on user identifier.

The auditable events include:

- Start-up and shutdown of the audit function (more specifically, of the TOE);
- Successful requests to perform an operation on an object covered by the SFP;
- Unsuccessful use of the authentication mechanism;
- Unsuccessful use of the user identification mechanism, including the user identity provided;

The TOE allows authorized administrators to define auditable events that can invoke user-defined logging modules (created by the authorized administrator) that are activated each time a client connects to the TOE. The TOE generates audit records which contain date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. Note that auditable events are associated with the identity of the user based on user identifier. The time is provided by the operating system in the IT environment.

The TOE writes audit records to text files stored in the IT environment that comprise the audit trail. The content server creates one file that contains start-up and shutdown and logon events; the security and logging server creates a second file that contains events for requests to perform operations on objects. The capability to audit access control decisions on database objects has to be set up using an ACE script and the “Event Hooks” mechanism. Access control events can be logged using the “onLocalPresentRecordFinal” event hook. The capability to define auditable events based on event hooks is specified in Section 5 – Logging and Events of the *Content Server User’s Guide.*

The operating system in the IT environment is relied on to protect audit trail files. The TOE does not provide any interfaces to read from the audit trail. Searching and sorting the audit trail would need to be performed using tools and interfaces of components in the IT environment such as UNIX shell scripts.

The User data protection function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE generates audit records for start-up and shutdown of the audit functions, as well as an unspecified level of audit. The TOE writes audit records to a text file stored in the IT environment.
- FAU_GEN.2: The TOE can generate audit events that include individual user identifiers.

6.1.2 User data protection

The TOE implements a Discretionary Access Control (DAC) SFP for object access based on:

- user identity,
- group memberships, and
- Permissions.

The TOE objects that are subject to this policy are Z39.50 databases, records, and elements.

- Z39.50 databases are conceptually equivalent to relational database tables, in that they consist of collections of related information that can be stored in a single logical data structure (a Z39.50 database).
- Z39.50 records are conceptually equivalent to relational database rows.
- Z39.50 elements are database record fields. Schema elements (or simply "elements") are conceptually equivalent to relational database row data that corresponds to a given column.

Note that there are two types of schema elements: simple record fields, and complex record fields. Simple record fields contain strings or integers and are normally directly bound to logical schema elements. Complex record fields contain, for example, XML content which may have multiple schema elements bound to other elements within the XML document.

The TOE implements a permissions mechanism that is relied on as follows to support the DAC SFP. The TOE is able to restrict access to TOE objects using permissions. Permissions are used to grant access to objects to users and groups. Users and groups that have been granted access to an object may access the object. Otherwise, access is denied, unless the user is a member of the DBA group, or if access is granted to all groups. Access to objects is defined in terms of the operations that a group may perform on the object. If the operation in the request is not supported for the object type, access is denied.

Groups can be granted or denied access to database objects for any combination of the following database operations:

- insert database records,
- update database records,
- delete database records, or
- query database records.

In order for a group to be granted insert, update, or delete access, the group must also be granted query access in order to perform insert, update, or delete operations.

Groups can be granted or denied access to element objects. Users and groups can be granted or denied access to record objects.

Element level security and row level security are specified at the access level, meaning that it is not possible to grant or deny permissions for query, insert, update, and delete separately.

An object can effectively be made public (i.e. members of any group may access the object) by specifying that all groups may be granted access.

One or more groups may be specified for a given object. If access is granted to one group and denied to another group and a user is a member of both groups, the "deny" takes priority and access is denied.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.1, FDP_ACF.1: All database subjects are subject to the DAC SFP for all available operations on Z39.50 databases, records, and elements.

6.1.3 Identification and authentication

The TOE defines users in terms of:

- user identity,
- authentication data, and
- group memberships.

The TOE provides its own username and password authentication mechanism. Note that while the product supports additional authentication mechanisms, only username/password is supported in the evaluated configuration. In order to access the TOE, a user account including a user name and password must be created for the user. User accounts can be assigned to administrator-defined groups, including a pre-defined DBA group. Members of the DBA group are considered authorized administrators, all others are simply users.

The TOE provides HTTP web form interfaces and API programmatic interfaces (both as identified in the TOE description) that can be used to access TOE services as well as manage TOE security functions as follows:

- interfaces to access TOE user services:
    - TeraText Advanced Search Interface Server – Users must enter username/password into a web form.
    - TeraText Command Line Interface Application – Users must enter username/password when prompted.
    - TeraText application programming interface (API) library – Users must enter username/password into API parameters.
- interfaces to manage TOE security functions:
    - TeraText Database Design Interface Server – Users must enter username/password into a web form.
    - TeraText Security and Logging Server – Users must enter username/password into a web form.
    - TeraText Directory Server – Users must enter username/password into a web form.
    - TeraText Boot Server – Users must enter username/password into a web form.
    - TeraText application programming interface (API) library – Users must enter username/password into API parameters.

The TeraText Security and Logging Server, TeraText Directory Server, and TeraText Boot Server authenticate users by establishing a TCP/IP socket connection to the TeraText Security and Logging Server, then sending an authentication request.

Each of the other above TeraText components and subcomponents authenticate the user attempting to login to the TOE by establishing a TCP/IP socket connection with the TeraText Content Server component, then sending an initialization request packet to identify information about the client (i.e. the above TeraText components and subcomponents) such as the name of the client application and its version number. The server then sends a response packet back with information about the server. A part of the request packet is a list of features that the client requests that the TeraText Content Server component support. The TeraText Content Server component responds with a list of features that the server can support. The client must then only use features that both the client and the server agreed to support. Note that the initialization request packet also includes a user name and password. Anonymous users are not supported in the evaluated configuration, so all users must be authenticated.

The TOE does not implement any password composition rules or minimum password lengths by default. Administrative guidance is relied on to provide configuration procedures that ensure when user accounts are created, a minimum password length of eight printable characters is used.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1: The TOE defines users in terms of user identity, authentication data, and group memberships.
- FIA_UAU.2: The TOE offers no TSF-mediated functions until the user is authenticated. Note that the password mechanism can meet or exceed SOF-basic when passwords of certain lengths are used.
- FIA_UID.2: The TOE offers no TSF-mediated functions until the user is identified.

6.1.4 Security management

The TOE defines the following user groups:

- DBA

Members of the DBA group can access all administrator console interfaces. The DBA group is a system-defined group. The TOE supports the following roles using the above-listed groups as follows:

- authorized administrators, and
- users.

Authorized administrators are users that are assigned to the DBA group. Users are all other users, including members of non-DBA administrator-defined groups (the TOE allows administrators to define groups).

Individual TOE components and subcomponents as identified in the security function description above provide web form GUI interfaces that are accessible using HTTP. Together, the set of individual component and subcomponent administrator GUIs comprise a single logical administrator console component. The administrator console interfaces can be used by administrators to perform the following:

- manage database users
- manage database objects
- session establishment
- audit functions

The TOE restricts access to its interfaces by requiring users to log into the administrator console component. The enforcement of subject or object attribute change shall take effect before the next access attempt on behalf of that subject

The TeraText Security and Logging Server provides interfaces to manage users. The TeraText Security and Logging Server can be used to change passwords using its web-based GUI interfaces as well as Ace programmatic interfaces. Note that typically programmatic interfaces called by applications in the IT environment provide interfaces that users can use to change their own passwords, the calling application would for example provide a GUI interface that would call the corresponding TeraText Security and Logging Server Ace interface. The TeraText Security and Logging Server can be used to create new accounts and manage user attributes using its web-based GUI interfaces as well as Ace programmatic interfaces. Users can be added, listed, edited, and removed.

The TeraText Database Design Interface Server provides interfaces to manage database objects, including: creating new databases and modifying existing databases.

The TeraText Database Design Interface Server can be used to grant or deny access to databases (equivalent to tables in a relational database) and elements (equivalent to columns in a relational database) to user groups. The DB Design Interface can be used to grant or deny access to databases and elements both when they are created and during operation using its web-based GUI interfaces as part of configuring database security settings. The DB Design Interface options for both grant or deny are “All” for all groups, “None” for no groups, and “Groups” for a specific list of user groups. The DB Design Interface allows separate query, insert, update, and delete permissions to be granted or denied to databases. For elements, only access permission is granted or denied. The use of DB Design Interface for granting or denying access to databases and elements is documented in Section 3.11 Database Security of the *Database Design Interface Guide*.

The Database Definition and Modification (DDM) language interface can be used to grant or deny access to groups using the DDM CREATE DATABASE or DDM ALTER DATABASE commands with the “query permissions”, “insert permissions”, “delete permissions”, and “update permissions” constructs. These are documented in *the Database Definition and Modification Reference Manual*.

Database and element security attributes can also be specified using the Database Design Language (DDL). Access can only be granted, but not denied, to the database using the DDL ALLOW command. The DDL ALLOW command is documented in Section 2.7 Allow: Defining Access Rights of the *Content Server Reference Manual*. The ALLOW option can also be used to specific element level security when defining the element within the DDL CREATE SCHEMA command. The DDL CREATE SCHEMA command is documented in Section 2.1 Create Schema: Logical Record Structure Definition of the *Content Server Reference Manual*.

Record (row) Level Security can only be specified using an ACE script. Since Record Level Security is specified using a script, access can be granted to an individual as well as to user groups. Guidance on writing an ACE script for record level security is provided in Section 9.5 – Record Level Security of the *Content Server User’s Guide.*

The Explain and Extended Services databases are also available to DBA users for managing and gathering information about the Content Server.

Configuration files that are shared between TeraText server components provide administrators with interfaces that can be used to manage TOE session establishment, including specifying IP addresses of originating client connections. The Security management function is designed to satisfy the following security functional requirements:

- FMT_MSA.1: The ability to manage subject and Z39.50 object attributes is restricted to an administrator by restricting access to administrative console interfaces.
- FMT_MSA.3: By default every object is created without any permissions being granted. There is no interface to change the default. .
- FMT_MTD.1a: The ability to set and reset subject authentication data is restricted to an authorized administrator or the user associated with the authentication data by restricting access to administrative console and network protocol interfaces.
- FMT_MTD.1b: The ability to manage TOE session establishment IP addresses is restricted to an authorized administrator by restricting access to administrative console interfaces.
- FMT_MTD.1c: The ability to manage the audit function is restricted to an authorized administrator by restricting access to administrative console interfaces.
- FMT_REV.1a: The ability to manage database subject attributes is restricted to an authorized administrator through discretionary access controls. This information is used to determine subject attributes each time a user connects to the TOE. However, when a subject attribute is revoked, the TOE ensures that the change is effective upon the next login. .
- FMT_REV.1b: The ability to manage database object attributes is restricted to an authorized administrator through discretionary access controls. The TOE ensures that the change is effective before the next access attempt related to that object.
- FMT_SMF.1: Administrators are able to perform all management functions, including: managing database subjects (including authentication data), objects, TOE session establishment, and the audit function using administrator console interfaces.
- FMT_SMR.1: Users that are members of the system-defined DBA group are considered authorized administrators, all others are simply users.

6.1.5 Protection of the TSF

The TOE instantiates itself as a process within task constructs provided by the underlying operating system. The TOE separates client connections to administrator console and client application components, and administrator console and client application component connections to the TeraText Content Server component. The TOE has been designed to provide well-defined interfaces that ensure access to protected resources is subject to applicable TOE implicit and explicit policies. The TOE also relies on its platform to operate correctly and to prevent unauthorized access to TOE data and stored executables.

- FPT_RVM.1a: The TOE prevents users from bypassing implicit and explicit policies that it enforces by controlling access to the administrator console and by controlling access to its non-administrative interfaces by requiring users to authenticate using username/password.
- FPT_SEP.1a: The TOE instantiates itself as a process which it protects from inappropriate access. The TOE separates clients based on individual protocol connections.

6.1.6 TOE access

The TOE can be configured to only accept client connections (of both users and authorized administrators) that originate from an administrator-configured list of originating IP addresses. For example, the TOE can be configured to only accept a client connection from the single deployed TeraText Advanced Search Interface Server component.

Users in this configuration would send/receive HTTP requests/responses to/from the TeraText Advanced Search Interface Server, which in turn would send/receive Z39.50 protocol messages to/from the TeraText Content Server component.

The Security management function is designed to satisfy the following security functional requirements:

- FTA_TSE.1: The TOE can restrict user sessions based on the IP address of the originating client connection.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by SAIC ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, life-cycle documentation, vulnerability analysis documentation, and configuration management documentation.

These activities are documented in:

- TeraText - Configuration Management Plan

The Configuration management assurance measure satisfies the following EAL 2 assurance requirements:

- ACM_CAP.2

6.2.2 Delivery and operation

SAIC provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary installation and generation instructions. SAIC delivery procedures describe all applicable procedures to be used to prevent inappropriate access to the TOE. SAIC also provides documentation that describes the steps necessary to install the TOE in accordance with the evaluated configuration.

These activities are documented in:

- TeraText - Delivery Procedures
- TeraText- Installation Manual
- TeraText - Common Criteria User’s Guide

The Delivery and operation assurance measure satisfies the following EAL 2 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

SAIC has numerous documents describing all facets of the design of the TOE. In particular, they have a functional specification that describes the accessible TOE interfaces; a high-level design that decomposes the TOE architecture into subsystems and describes each subsystem and their interfaces; and, correspondence documentation that explains how each of the design abstractions correspond from the TOE summary specification in the Security Target to the subsystems.

These activities are documented in:

- TeraText - Design Document (HLD, FSP, and RCR),
- TeraText DBS Patch 4_3_13 Notes.htm

The Development assurance measure satisfies the following EAL 2 assurance requirements:

- ADV_FSP.1
- ADV_HLD.1
- ADV_RCR.1

6.2.4 Guidance documents

SAIC provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

TeraText Database System Release 4.3, Administrator Manual Series:

- Administration Manual
- Application Server Reference Manual
- Application User's Guide
- Boot Server User's Guide
- Common Criteria User's Guide
- Content Server Reference Manual
- Content Server User's Guide
- Database Definition and Modification Reference Manual
- Directory Server User's Guide
- Getting Started
- Installation Manual
- Security and Logging Server User's Guide

TeraText Database System Release 4.3, User Manual Series:

- Advanced Search Interface User's Guide
- Command Line Interface User's Guide
- Database Design Interface User's Guide

The Guidance documents assurance measure satisfies the following EAL 2 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Tests

SAIC has a test plan that describes how each of the necessary security functions is tested, along with the expected test results. SAIC has documented each test as well as an analysis of test coverage and depth demonstrating that the security aspects of the design evident from the functional specification and high-level design are appropriately tested. Actual test results are also provided to demonstrate that the tests have been applied and that the TOE operates as designed.

These activities are documented in:

- TeraText - Test Document (COV and FUN)
- TeraText - Test Scripts

The Tests assurance measure satisfies the following EAL 2 assurance requirements:

- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2

6.2.6 Vulnerability assessment

SAIC has conducted a strength of function analysis wherein all permutational or probabilistic security mechanisms have been identified and analyzed resulting in a demonstration that all of the relevant mechanisms fulfill the minimum strength of function claim, SOF-Basic.

SAIC performs regular vulnerability analyses of the entire TOE (including documentation) to identify obvious weaknesses that can be exploited in the TOE.

These activities are documented in:

- TeraText - Vulnerability Analysis Report

The Vulnerability assessment assurance measure satisfies the following EAL 2 assurance requirements:

- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

There is no Protection Profile claim in this ST.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives.

	P.ACCOUNTABILITY	P.AUTHORIZATION	P.AUTHORIZED_USERS	P.I_AND_A	P.NEED_TO_KNOW	P.ROLES	T.ADMIN_ERROR	T.AUDIT_COMPROMISE	T.MASQUERADE	T.SYSACC	T.TSF_COMPROMISE	T.UNAUTH_ACCESS	T.UNDETECTED_ACTIONS	T.UNIDENTIFIED_ACTIONS	A.NO_EVIL	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A. ENVIRONMENT	A.NETWORK
O.ACCESS		X	X		X					X		X							
O.ADMIN_ROLE						X													
O.AUDIT_GENERATION	X							X					X						
O.DISCRETIONARY_ACCESS					X							X							
O.INTERNAL_TOE_DOMAINS												X							
O.MANAGE							X			X									
O.PROTECT		X			X							X							
O.TOE_PROTECTION											X								
O.USER_AUTHENTICATION				X					X	X									
O.USER_IDENTIFICATION	X	X		X	X				X	X									
OE.AUDIT_PROTECTION								X					X						
OE.AUDIT_REVIEW	X													X					
OE.TIME	X												X						
OE.TOE_PROTECTION											X								
OE.PERSON							X			X									
OE.CONFIG															X				
OE.INSTALL							X												
OE.NO_GENERAL_PURPOSE																X			
OE.PHYSICAL								X		X	X	X	X				X		
OE.SELF_PROTECTION								X				X							X
OE.TRUST_IT																		X	

Table 4 Environment to Objective Correspondence

8.1.1.1 P.ACCOUNTABILITY

The users of the TOE shall be held accountable for their actions within the TOE.

This Organizational Policy is satisfied by ensuring that:

- O.AUDIT_GENERATION: Enforcement of this policy requires all user logon actions be recorded.
- O.USER_IDENTIFICATION: The TOE will uniquely identify all users.
- OE.AUDIT_REVIEW: The IT environment must provide the ability to review all recorded actions by the authorized administrator.
- OE.TIME: The IT environment must provide a reliable time source for the TOE to provide an accurate timestamp for all audit records ensuring.

8.1.1.2 P.AUTHORIZATION

The abilities of users of the TOE shall be limited in accordance with the TSP.

This Organizational Policy is satisfied by ensuring that:

- O.ACCESS: The TOE will ensure that access control decisions are enforced based on the applicable user and data security attributes and that administrators can manage user attributes.
- O.PROTECT: The TOE will ensure that access control decisions are enforced based on the applicable user and data security attributes and that users can manage access to their own data.

- O.USER_IDENTIFICATION: The TOE will uniquely identify each user.

8.1.1.3 P.AUTHORIZED_USERS

Access controls will ensure that only those users who have been authorized to access the protected information within the TOE will be able to do so.

This Organizational Policy is satisfied by ensuring that:

- O.ACCESS: The TOE will provide mechanisms to allow only authorized users to access the TOE, mainly Discretionary Access Controls.

8.1.1.4 P.I_AND_A

All users must be identified and authenticated prior to accessing any controlled resources.

This Organizational Policy is satisfied by ensuring that:

- O.USER_AUTHENTICATION: The TOE requires users to authenticate their identity prior to accessing any other functions.
- O.USER_IDENTIFICATION: The TOE requires users to claim their unique identity prior to accessing any other functions.

8.1.1.5 P.NEED_TO_KNOW

The users of the TOE shall limit the access to information in protected resources to those authorized users who have a need to know that information.

This Organizational Policy is satisfied by ensuring that:

- O.ACCESS: The TOE provides the authorized administrator functions to change a user's security attributes when that user no longer needs to access certain information.
- O.DISCRETIONARY_ACCESS: The TOE requires the resources to be protected according to the rules of the discretionary access control policy.
- O.PROTECT: The TOE requires the protection of user data and resources.
- O.USER_IDENTIFICATION: The TOE requires access decision to be based on unique user identities.

8.1.1.6 P.ROLES

The users of the TOE shall use an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

This Organizational Policy is satisfied by ensuring that:

- O.ADMIN_ROLE: The TOE has the objective of providing an authorized administrator role for secure administration. The TOE may provide other roles as well, but only the role of authorized administrator is required.

8.1.1.7 T.ADMIN_ERROR

An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

This Threat is satisfied by ensuring that:

- O.MANAGE: The TOE provides the administrator the necessary security management functions.
- OE.PERSON: The TOE guidance includes complete and clear administration guidance.
- OE.INSTALL: The TOE guidance includes the necessary installation instructions that detail how to securely install the TOE.

8.1.1.8 T.AUDIT_COMPROMISE

A process or user may cause audit data to be inappropriately accessed (viewed, modified or deleted), or prevent future records from being recorded, thus masking an attacker's actions.

This Threat is satisfied by ensuring that:

- O.AUDIT_GENERATION: Enforcement of this policy requires all user logon actions be recorded.
- OE.AUDIT_PROTECTION: The IT environment must also provide protection for the audit data.
- OE.PHYSICAL: The environment must address the possible compromise of audit data due to physical means.
- OE.SELF_PROTECTION: The IT environment must also protect itself and its assets.

8.1.1.9 T.MASQUERADE

An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.

This Threat is satisfied by ensuring that:

- O.USER_AUTHENTICATION: The TOE requires all users of the TOE to prove their claimed unique identity.
- O.USER_IDENTIFICATION: The TOE uniquely identifies each user.

8.1.1.10 T.SYSACC

A malicious process or user may gain unauthorized access to the authorized administrator account, or that of other trusted personnel.

This Threat is satisfied by ensuring that:

- O.ACCESS: The TOE prevents the wrong individuals from gaining unauthorized access to the authorized administrator’s account.
- O.MANAGE: The TOE provides mechanisms for the authorized administrator to set the security attributes for users so they are not allowed admin access.
- O.USER_AUTHENTICATION: The TOE requires the authorized administrator to be authenticated.
- O.USER_IDENTIFICATION: The TOE requires the authorized administrator to be uniquely identified.
- OE.PERSON: The TOE guidance includes complete and clear administration guidance.
- OE.PHYSICAL: The environment must address the possible unauthorized access to administrative accounts due to physical means.

8.1.1.11 T.TSF_COMPROMISE

An unauthorized user may gain access to the TOE and cause configuration data to be inappropriately accessed (viewed, modified or deleted).

This Threat is satisfied by ensuring that:

- O.TOE_PROTECTION: The TOE protects TSF data and executable code.
- OE.TOE_PROTECTION: The IT environment will provide protection to the TOE and its assets from external interference or tampering.
- OE.PHYSICAL: The environment must protect the TSF data and executable code from a compromise through physical means.

8.1.1.12 T.UNAUTH_ACCESS

A user may gain unauthorized access (view, modify, delete) to user data.

This Threat is satisfied by ensuring that:

- O.ACCESS: The TOE ensures that only authorized users may gain access to the TOE and the resources it protects, and that users are not allowed to access protected data for which they are not authorized.
- O.DISCRETIONARY_ACCESS: The TOE controls access to user data by a discretionary access control policy.
- O.INTERNAL_TOE_DOMAINS: The TOE maintains internal domains to keep data and processes of concurrent users separate, so users cannot observe or interfere with other users’ data or queries.

- O.PROTECT: The TOE prevents unauthorized access to user data.
- OE.PHYSICAL: The environment must prevent unauthorized physical access to the TOE.
- OE.SELF_PROTECTION: The environment must prevent unauthorized physical to itself.

8.1.1.13 T.UNDETECTED_ACTIONS

Unauthorized attempts to access TOE data or security functions may go undetected..

This Threat is satisfied by ensuring that:

- O.AUDIT_GENERATION: Enforcement of this policy requires all user logon actions be recorded.
- OE.AUDIT_PROTECTION: The IT environment prevents unauthorized modification of audit records
- OE.TIME: The IT environment must provide a reliable time source for the TOE to provide an accurate timestamp for all audit records ensuring.
- OE.PHYSICAL: The environment must prevent potentially undetected physical manipulation of the TOE.

8.1.1.14 T.UNIDENTIFIED_ACTIONS

An authorized administrator may not be able to read audit records stored in the audit trail

This Threat is satisfied by ensuring that:

- OE.AUDIT_REVIEW: The IT environment must provide the ability to review all recorded actions by the authorized administrator.

8.1.1.15 A.NO_EVIL

Authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.

This Assumption is satisfied by ensuring that:

- OE.CONFIG: Authorized administrators are trained and trusted to properly configure the IT environment so it enforces its security policies.

8.1.1.16 A.NO_GENERAL_PURPOSE

There are no general-purpose computing capabilities (e.g., compilers or user applications) available on TOE servers, other than those services necessary for the operation, administration and support of the TOE.

This Assumption is satisfied by ensuring that:

- OE.NO_GENERAL_PURPOSE: The TOE server must not include any general-purpose commuting or storage capabilities. This will protect the TSF data from malicious processes.

8.1.1.17 A.PHYSICAL

It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.

This Assumption is satisfied by ensuring that:

- OE.PHYSICAL: The environment in which the TOE operates is sufficient for secure operation. That the parts of the TOE critical to security policy are protected from physical attack and modification that might compromise the TOE security objectives.

8.1.1.18 A. ENVIRONMENT

It is assumed that the IT environment provides support commensurate with the expectations of the TOE.

This Assumption is satisfied by ensuring that:

- OE.TRUST_IT: The IT entities in the environment are correctly installed, configured, managed, maintained and provide the applicable security functions.

8.1.1.19 A.NETWORK

It is assumed that the environment protects network communication media appropriately.

This Assumption is satisfied by ensuring that:

- OE.SELF_PROTECTION: The IT environment must also protect itself and its assets.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 5** indicates the requirements that effectively satisfy the individual objectives. .

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.ACCESS	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.DISCRETIONARY_ACCESS	O.INTERNAL_TOE_DOMAINS	O.MANAGE	O.PROTECT	O.TOE_PROTECTION	O.USER_AUTHENTICATION	O.USER_IDENTIFICATION	OE.AUDIT_PROTECTION	OE.AUDIT_REVIEW	OE.TIME	OE.TOE_PROTECTION
FAU_GEN.1			x											
FAU_GEN.2			x											
FAU_SAR.1												x		
FAU_STG.1											x			
FDP_ACC.1	x			x			x							
FDP_ACF.1	x			x			x							
FIA_ATD.1										x				
FIA_UAU.2									x					
FIA_UID.2										x				
FMT_MSA.1				x		x								
FMT_MSA.3						x								
FMT_MTD.1a						x			x					
FMT_MTD.1b	x					x								
FMT_MTD.1c	x					x								
FMT_REV.1a	x													
FMT_REV.1b							x							
FMT_SMF.1				x		x								
FMT_SMR.1		x												
FPT_RVM.1a					x			x						
FPT_RVM.1b														x
FPT_SEP.1a					x			x						
FPT_SEP.1b														x

FPT_STM.1			x										x	
FTA_TSE.1	x													

Table 5 Objective to Requirement Correspondence

8.2.1.1 O.ACCESS

The TOE will ensure that users gain only authorized access to it and to the resources that it controls.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.1: All database subjects are subject to the DAC SFP for all available operations on Z39.50 databases, records, and elements.
- FDP_ACF.1: The TOE is able to restrict access to databases, records, and elements using permissions. Permissions are used to grant access to objects to users and groups. Users who are identified as members of groups that have been granted access to an object may access the object.
- FMT_REV.1a: The ability to manage database subject attributes is restricted to an authorized administrator through discretionary access controls. This information is stored in configuration files stored in the IT environment. This information is used to determine subject attributes each time a user connects to the TOE. However, when a subject attribute is revoked, the TOE ensures that the change is effective before the next access attempt on behalf of the subject.
- FMT_MTD.1b: The ability to manage TOE session establishment IP addresses is restricted to an authorized administrator by restricting access to administrative console interfaces.
- FMT_MTD.1c: The ability to manage the audit function is restricted to an authorized administrator by restricting access to administrative console interfaces..
- FTA_TSE.1: The TOE can restrict user sessions based on the IP address of the originating client connection.

8.2.1.2 O.ADMIN_ROLE

The TOE will provide authorized administrator roles to isolate administrative actions.

This TOE Security Objective is satisfied by ensuring that:

- FMT_SMR.1: Users that are members of the system-defined DBA group are considered authorized administrators, all others are simply users.

8.2.1.3 O.AUDIT_GENERATION

The TOE will provide the capability to detect and create records of security relevant events associated with users.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: The TOE can generate audit events for the minimum level of audit are recorded in audit trail files stored in the IT environment.
- FAU_GEN.2: The TOE can generate audit events that include individual user identifiers.
- FPT_STM.1: Reliable time stamps are assumed to be provided by the IT environment.

8.2.1.4 O.DISCRETIONARY_ACCESS

The TOE will control access to resources based upon the identity of users, group membership of users, and access control lists.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.1: All database subjects are subject to the DAC SFP for all available operations on Z39.50 databases, records, and elements.

- FDP_ACF.1: The TOE is able to restrict access to databases, records, and elements using permissions. Permissions are used to grant access to objects to users and groups. Users who are identified as members of groups that have been granted access to an object may access the object.
- FMT_MSA.1: The ability to manage Z39.50 object attributes is restricted to an administrator by restricting access to administrative console interfaces.
- FMT_SMF.1: Administrators are able to perform all management functions, including: managing database subjects (including authentication data) and objects using administrator console interfaces.

8.2.1.5 O.INTERNAL_TOE_DOMAINS

The TSF will maintain internal domains for separation of data and queries belonging to concurrent users.

This TOE Security Objective is satisfied by ensuring that:

- FPT_RVM.1a: The TOE prevents users from bypassing implicit and explicit policies that it enforces by controlling access to the administrator console and by controlling access to its non-administrative interfaces by requiring users to authenticate using username/password.
- FPT_SEP.1a: The TOE instantiates itself as a process which it protects from inappropriate access. The TOE separates clients based on individual protocol connections.

8.2.1.6 O.MANAGE

The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MSA.1: The ability to manage subject and Z39.50 object attributes is restricted to an administrator by restricting access to administrative console interfaces.
- FMT_MSA.3: By default every object is created without any permissions. Subsequently, access can be granted to other users.
- FMT_MTD.1a: The ability to set and reset subject authentication data is restricted to an authorized administrator or the user associated with the authentication data by restricting access to administrative console and network protocol interfaces.
- FMT_MTD.1b: The ability to manage TOE session establishment IP addresses is restricted to an authorized administrator by restricting access to administrative console interfaces.
- FMT_MTD.1c: The ability to manage the audit function is restricted to an authorized administrator by restricting access to administrative console interfaces.
- FMT_SMF.1: Administrators are able to perform all management functions, including: managing database subjects (including authentication data), objects, and TOE session establishment using administrator console interfaces.

8.2.1.7 O.PROTECT

The TOE will provide mechanisms to protect user data and resources.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.1: All database subjects are subject to the DAC SFP for all available operations on Z39.50 databases, records, and elements.
- FDP_ACF.1: The TOE is able to restrict access to databases, records, and elements using permissions. Permissions are used to grant access to objects to users and groups. Users who are identified as members of groups that have been granted access to an object may access the object.
- FMT_REV.1b: The ability to manage database object attributes is restricted to an authorized administrator through discretionary access controls. The TOE ensures that the change is effective before the next access attempt related to that object.

8.2.1.8 O.TOE_PROTECTION

The TOE will protect itself and its assets from external interference or tampering.

This TOE Security Objective is satisfied by ensuring that:

- FPT_RVM.1a: The TOE prevents users from bypassing implicit and explicit policies that it enforces by controlling access to the administrator console and by controlling access to its non-administrative interfaces by requiring users to authenticate using username/password.
- FPT_SEP.1a: The TOE instantiates itself as a process which it protects from inappropriate access. The TOE separates clients based on individual protocol connections.

8.2.1.9 O.USER_AUTHENTICATION

The TOE will verify the claimed identity of users.

This TOE Security Objective is satisfied by ensuring that:

- FIA_UAU.2: The TOE offers no TSF-mediated functions until the user is authenticated.
- FMT_MTD.1a: The ability to set and reset subject authentication data is restricted to an authorized administrator or the user associated with the authentication data by restricting access to administrative console and network protocol interfaces.

8.2.1.10 O.USER_IDENTIFICATION

The TOE will uniquely identify users.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1: The TOE defines users in terms of user identity, authentication data, and group memberships.
- FIA_UID.2: The TOE offers no TSF-mediated functions until the user is identified.

8.2.1.11 OE.AUDIT_PROTECTION

The IT Environment will provide the capability to protect audit information.

This IT Environment Security Objective is satisfied by ensuring that:

- FAU_STG.1: The IT Environment prevents unauthorized deletion or modification of audit records.

8.2.1.12 OE.AUDIT_REVIEW

The IT environment will provide the capability to view audit information, and alert the authorized administrator of identified potential security violations.

This IT Environment Security Objective is satisfied by ensuring that:

- FAU_SAR.1: The IT Environment provides the ability to review audit records.

8.2.1.13 OE.TIME

The IT environment will provide a time source that provides reliable time stamps.

This IT Environment Security Objective is satisfied by ensuring that:

- FPT_STM.1: The IT environment is required to provide a reliable time source.

8.2.1.14 OE.TOE_PROTECTION

The IT environment will provide protection to the TOE and its assets from external interference or tampering.

This IT Environment Security Objective is satisfied by ensuring that:

- FPT_RVM.1b: The IT environment ensures the TOE can only be accessed using its interfaces.
- FPT_SEP.1b: The IT environment is required to maintain separation between calling user processes.

8.3 Security Assurance Requirements Rationale

EAL2 was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate degree of independently assured security. SAIC TeraText DBS 4.3.13 is targeted at a relatively benign environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have little attack potential. As such, EAL2 is appropriate to provide the assurance necessary to counter the limited potential for attack.

8.4 Strength of Functions Rationale

The overall strength of function claim of basic is believed to be commensurate with the overall assurance claim of EAL 2. The only applicable security function is Identification and Authentication. The password mechanism is used in the Identification and Authentication security function to authenticate user identity. The relevant security functional requirement is FIA_UAU.2. The intent is that the password mechanism meets or exceeds SOF-basic and the evidence can be found in the strength of function analysis included in SAIC TeraText DBS 4.3.13 Vulnerability Analysis.

8.5 Requirement Dependency Rationale

The following table demonstrates that all dependencies among the claimed security requirements are satisfied and therefore the requirements work together to accomplish the overall objectives defined for the TOE.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 and FIA_UID.1	FAU_GEN.1 and FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.1 and FMT_MSA.3
FIA_ATD.1	NONE	NONE
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	NONE	NONE
FMT_MOF.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MSA.1	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_ACC.1
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1 and FMT_SMR.1
FMT_MTD.1a	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1b	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1c	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_REV.1a	FMT_SMR.1	FMT_SMR.1
FMT_REV.1b	FMT_SMR.1	FMT_SMR.1
FMT_SMF.1	NONE	NONE
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_RVM.1a	NONE	NONE
FPT_RVM.1b	NONE	NONE
FPT_SEP.1a	NONE	NONE
FPT_SEP.1b	NONE	NONE
FPT_STM.1	NONE	NONE
FTA_TSE.1	NONE	NONE
ACM_CAP.2	NONE	NONE
ADO_DEL.1	NONE	NONE
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1
ADV_HLD.1	ADV_FSP.1 and ADV_RCR.1	ADV_FSP.1 and ADV_RCR.1

ADV_RCR.1	NONE	NONE
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1	ADV_FSP.1
ATE_COV.1	ADV_FSP.1 and ATE_FUN.1	ADV_FSP.1 and ATE_FUN.1
ATE_FUN.1	NONE	NONE
ATE_IND.2	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1
AVA_SOF.1	ADV_FSP.1 and ADV_HLD.1	ADV_FSP.1 and ADV_HLD.1
AVA_VLA.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1

Table 6 Security Functions Dependency Mapping

8.6 Explicitly Stated Requirements Rationale

There are no explicitly stated requirements.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 7 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security audit	**User data protection**	**Identification and authentication**	**Security management**	**Protection of the TSF**	**TOE access**
FAU_GEN.1	x					
FAU_GEN.2	x					
FDP_ACC.1		x				
FDP_ACF.1		x				
FIA_ATD.1			x			
FIA_UAU.2			x			
FIA_UID.2			x			
FMT_MSA.1				x		
FMT_MSA.3				x		
FMT_MTD.1a				x		
FMT_MTD.1b				x		
FMT_MTD.1c				x		
FMT_REV.1a				x		
FMT_REV.1b				x		
FMT_SMF.1				x		
FMT_SMR.1				x		

FPT_RVM.1a					x	
FPT_SEP.1a					x	
FTA_TSE.1						x

Table 7 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.