IBM DB2® Content Manager for Multiplatforms V8.2 Security Target

ST Version 1.0

22 November 2004

Prepared For:

International Business Machines (IBM)
555 Bailey Avenue
San Jose, CA 95161

Prepared By:

Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Gateway Drive
Columbia, MD 21046

1 Security Target (ST) Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE). Specifies the ST conventions, terminology, and acronyms, and ST conformance claims; and describes the ST organization.

1.1 Security Target, TOE, and Vendor Identification

ST Title – IBM DB2® Content Manager for Multiplatforms v8.2 Security Target

ST Version – 1.0

TOE Identification – IBM DB2® Content Manager for Multiplatforms v8.2 + fix pack 6 for Sun Solaris 2.8, AIX® 5.1, Windows® 2000, and Windows XP

IBM DB2® Content Manager for Multiplatforms v8.2 GA for Linux RedHat 3.0, Linux SUSE 8

IBM DB2® Content Manager for Multiplatforms v8.2 + PTF UQ89832 for z/OS v1.3

Vendor – IBM

Evaluation Assurance Level (EAL) – EAL 3 augmented with ALC_FLR.1

1.2 Common Criteria Conformance Claims

This TOE and ST are consistent with the following specifications:

- Common Criteria (CC) for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.1, August 1999, ISO/IEC 15408-2
  - Part 2 conformant
- Common Criteria (CC) for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.1, August 1999, ISO/IEC 15408-3
  - Part 3 conformant
  - Evaluation Assurance Level 3 (EAL3) augmented with ALC_FLR.1
- The ST claims a minimum strength of function of SOF-Basic for the TOE.

1.3 Conventions, Terminology, and Acronyms

1.3.1 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 in parenthesis placed at the end of the component. For example FCS_COP.1(a) and FCS_COP.1(b) indicate that the ST includes two iterations of the FCS_COP.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 "…**big** ~~some~~ things …").

- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Terminology

The terminology used in this Security Target is defined below:

Authorized users	The users, administrative and non-administrative, who have been give access to the TOE.
Connectors	Object-oriented programming class that provides standard access to APIs native to specific content servers.
Event log	An audit record in the event tables.
Privilege set	A group of privileges that can be assigned to a user.
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Target of Evaluation (TOE)	An IT product of system and its associated guidance documentation that is the subject of an evaluation.
User Group	A group of individual users who perform similar tasks.
Resource	Any data entity that is stored on a resource manager in digital form. Objects can include, but are not limited to, JPEG images, MP3 audio, AVI video, or a plain text file. For example, a few of the formats that are supported natively by Content Manager are: Microsoft Word, Lotus® WordPro, TIFF, and JPEG.

1.3.3 Acronyms

The acronyms used within this Security Target are expanded below:

ACL	Access Control Lists
CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
IT	Information Technology
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control

TSF	TOE Security Functions
TSP	TOE Security Policy

1.4 Security Target Overview and Organization

This IBM Content Manager Security Target describes the IBM DB2® Content Manager. IBM DB2® Content Manager is a database and data management system (content management system) that provides a foundation for managing, accessing, and integrating critical business information on demand.

The security target is organized as follows:

- 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 and the organizational policy that must fulfill.

- Section 4 – TOE Security Objectives

  This section details the security objectives of the TOE and its environment.

- Section 5 – IT Security Requirements

  The section presents the security functional requirements (SFR) for TOE and IT Environment that supports the TOE, and details the assurance requirements for EAL3 augmented.

- Section 6 – TOE Summary Specification

  The section describes the security functions represented in the TOE 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.

2 Target of Evaluation (TOE) Description

The TOE is the IBM DB2® Content Manager for Multiplatforms V8.2, henceforth referred to as Content Manager.

2.1 Product Type

Content Manager is a data management system (content management system) that provides a foundation for managing, accessing, and integrating critical business information on demand. Content Manager is able to integrate all forms of data — document, Web, image, rich media — across diverse business processes and applications, including Siebel, PeopleSoft, and SAP, presenting the data in a integrated context for later use.

2.2 Product Description

The main components of the Content Manager include a Library Server, one or more Resource Managers, Client for Windows, System Administration Client, and a set of object-oriented application programming interfaces (APIs). Additionally, to administer Content Manager, an administrator is provided with a system administration client.

- The Library Server is the key component of the Content Manager system. The Library Server resides on a DB2 Universal Database environment. It is called the Library Server because it performs the functions that a library catalog file in a real library performs. The Library Server manages the content metadata (resources) and is responsible for identification and authentication for non-administrative users and identification for administrative users requesting services from Content Manager and access control to the resources residing on Resource Managers. The Library Server manages the relationships between items in the system and controls access to all of the system information, including the information stored in the Resource Managers. The Library Server processes requests (like update or delete) from one or more clients. A Content Manager system requires one Library Server, which can run on the Windows, AIX, or Solaris operating system. In Content Manager, all access to the Library Server is via the database query language, SQL. The Library Server code is co-resident with the DB2 database engine code. The Library server passes back to the client query results that include security tokens and locators for requested content that the user is authorized to access. The DB2 Universal Database is not part of the TOE.
- The Resource Manager stores resources for Content Manager. It can be on the same workstation as the Library Server, or it can be on its own computer. Resource managers can be distributed across networks to provide convenient user access. Users store and retrieve digital resources on the Resource Manager by routing requests through the Library Server. A single Library Server can support multiple Resource Managers and content can be stored on any of these Resource Managers. When the Library Server grants an access request, the Library Server returns a security token and the location of the object to the users. Data objects are always associated with a specific collection on a Resource Manager. Access decisions to grant access to a collection of data objects are made by the Library Server. The Resource Manager enforces access decisions. The client communicates directly with the Resource Manager using Internet protocols. Security tokens received from the Library Server are passed to Resource Managers from a client to provide assurance that the request has been authorized and the access control information has not been altered since leaving the Library Server.
- The System Administration Client oversees the entire Content Manager system. From the system administration client, an administrator performs various administrative functions, such as define the data model, creating users and defining their access to the system and specific objects, and managing storage and storage objects in the system. The System Administration Client can be installed on any workstation with the other components or on its own workstation.

- The Client for Windows provides an interface that enables an application to import documents into Content Manager, view them, work with them, store them, and retrieve them. The APIs associate with the Client are part of the TOE.
- The Web Application Server interface for the Resource Manager is typically another IBM product, WebSphere. The Web Application Server provides the Resource Manager access to web applications as a requested resource. A set of object-oriented APIs utilized by the TOE reside on the Web Application Server. The Web Application Server and the APIs are not included in the TOE however the Web Application Server interface is an external interface into part of the TSF (Resource Manager).

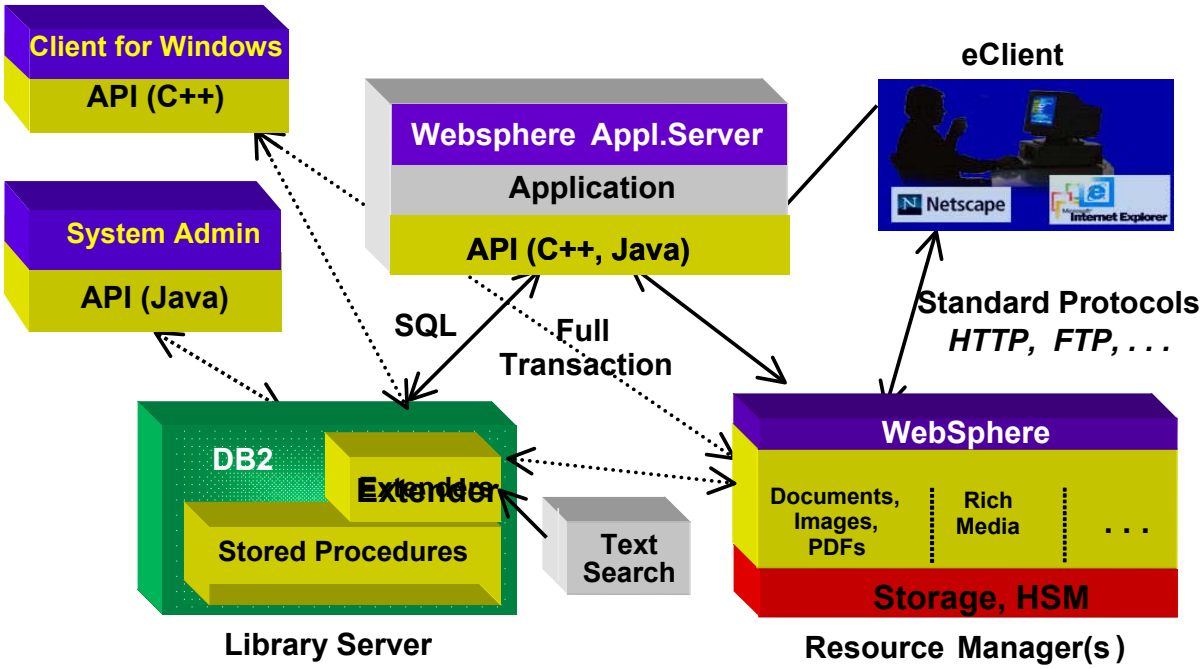

Figure 1: Content Manager Architecture

2.3 Product Features

Content Manager supports multiple operating systems, and applications.

- The servers can run on the Sun Solaris 2.8, AIX® 5.1, Linux RedHat 3.0, Linux SUSE 8, z/OS v1.3, and Windows® 2000 environments.
- The System Administration client can run on Windows® 2000, Windows XP, and Linux RedHat 3.0 and Linux SUSE 8 environments.
- The client can run on Windows® 2000, and Windows® XP environments.
- Based on industry standards and Internet protocols, the system is also designed to be fully open to any application.

- The multi-tier distributed architecture and logical separation of applications, indices, and data provides application independence from any changes in the location of data.

Powerful embedded database engine

- All library server logic in Content Manager runs within DB2 Universal Database. In effect, this architecture implements a data model within the relational database engine that is more appropriate for managing unstructured information than the relational model of tables, rows and columns. Sophisticated stored procedures map the data model without executing logic in the client or a mid-tier application. Thus, applications built on this new model do not pay the performance penalty that an intermediate mapping layer requires. Equally important, the new data model inherits many key values and attributes of the mature relational system, like transactional and data integrity.

Advanced data modeling capability

- Content Manager acts as the central authority for correlating diverse terms used for the same business attribute and for simplifying navigation and access to information for all authorized users and applications.
- Content Manager stores and manages indexing attributes in its library server, whereas objects are stored and managed in one or more associated resource managers. The following object attributes are managed:
    - Relationships to other objects
    - Access control, including who can access the object and the actions that authorized users can perform
    - Storage profile for hierarchical storage management
    - Lifecycle and retention
    - Workflow initiation, process integration and automation

Flexible data model

- The Content Manager data model is very flexible and supports hierarchical structures such as parent-child and peer-to-peer relationships.
- Attributes for an object can be structured with parent and child relationships that match the hierarchical structure in real-world customer application environments.
- It allows the creations of objects that combine attributes from different business processes and centralize information as needed.

Peer-to-peer relationships: links and references

- Content Manager allows custom applications to build more complex inter-object peer-to-peer relationships using links and references.

  Links have the following characteristics:

    - A link type can model a many-to-many relationship. In other words, an item can be linked with multiple items.
    - Content Manager manages links separately from items, allowing for flexible application designs.

- The semantics of a link are directional, with a source and a target, so a link can be traversed bi-directionally very efficiently.
- A link is version-independent. It can be traversed to get the latest, a specific, or all versions of the linked document. For compound document and Web content applications, this feature supports the flexibility to specify whether linked items should retain their relationships with the existing version, or update to reflect the most recent version of the various items that make up the compound document.

The Content Manager supports the folder-contains link, which supports folder hierarchy and allows users to define additional custom link types to meet specific needs within custom applications.

References allows a reference pointer from any component in an item hierarchy to any item of any type in the system to maintain referential integrity of item relationships by following DB2 Universal Database delete rules.

- In Content Manager, applications can also define attributes as foreign keys to external DB2 Universal Database tables that are not part of the Content Manager schema. This capability allows applications to associate with other DB2 Universal Database applications and to help ensure referential integrity with external data.

Version control

- Content Manager supports the storage of multiple versions of documents and parts within documents. Content Manager can create a new version when any changes occur in the document content or in its indexing attributes. Each version of a document is stored as a separate item in the system. Users can access the latest version or any version of the document by specifying the desired version number. To limit the number of versions managed in the system, administrators configure how many versions exist for a single item. Content Manager automatically deletes older versions exceeding the limit.
- The authorized administrator can determine, by item type, whether a store or update operation creates a version, modifies the latest version or prompts the user to create a version.

Search and access

Content Manager provides advanced search and access technologies that give users the ability to locate and retrieve content quickly and accurately.

Content Manager uses three search methods: parametric search, full-text search and combined parametric and full-text search.

- Parametric search lets you locate the contents by specifying criteria based on metadata attributes.
- Full-text search allows the entry of free text or keywords as search criteria against text-indexed documents to locate documents that contain pertinent content anywhere within the body of the document.
- Combined parametric and full-text search allows users to enter both metadata attributes and full-text or keywords to expand search criteria.

Enterprise-wide content integration

- Content Manager provides an integrated information framework for single-point access to all heterogeneous systems of content repositories.

- Content Manager includes content connectors to enable access to a broad range of IBM repositories, and allows connectors to be constructed for new target systems to support searching in both IBM and non-IBM content repositories as needed.
- Content Manager provides a federated connector as the common interface for content in multiple applications. The federated connector accesses individual connectors to allow any content sources (including non-IBM products) to be accessed with common APIs and components.

Distributed and hierarchical storage management

- Content Manager allows migration of objects from one resource manager to another. It also allows automatic object migration when business growth demands an upgrade to a new hardware platform or when a physical move warrants object migration to remote servers.
- The resource managers can be distributed in geographically dispersed locations within an enterprise for faster access to frequently referenced objects.
- In addition to traditional objects such as text documents and production images, a resource manager can also store and manage a growing spectrum of digital content -- from static archives to dynamic content -- including scanned images, facsimiles, PC files, XML, audio, video, streaming video, and web content

2.4 Scope of TOE

2.4.1 Physical Boundary

The physical boundaries of the TOE are defined by the operating system that each component of the TOE requires for effective operation. The TOE is a database software application that is comprised of the applications required for the correct enforcement of the security functions. The TOE utilizes an embedded database, DB2 Universal Database, which is part of the environment.

2.4.2 Logical Boundary

The logical boundaries of the TOE can be described in the terms of the security functions.

2.4.2.1 Audit Function

All security-related events within Content Manager are logged. These are tied to the user/administrator that performed the action, as well as the action performed, and the time it was performed. These audit records are stored in a central location where an authorized administrator can review them. Authorized non-administrative users can review the audit records generated for resources that they have been granted access. The IT environment provides the tools that are utilized by the TOE users to review the audit records.

2.4.2.2 Identification and Authentication

Content Manager requires the user to be identified and authenticated before any other actions can be performed. The user is required to provide a user name and password, which will be verified by the Library Server database table. If the verification is successful access into the TOE is granted.

2.4.2.3 User Data Protection

Access to the resources and its information is governed by the object's ACL that identifies the user and the privileges allowed. The Library Server verifies that the user has the required privilege and the ACL associated to the requested object grants access.

2.4.2.4 Security Management

System Administration Clients provides the authorized administrator the capability to manage the security-related functions and attributes, such as the audit function, management of users and their associated data.

2.4.2.5 Protection of the TSF

Content Manager provides various mechanisms to protect the TSF data in transmit and to enforce the access control policy ensuring that only authorized users with the appropriate privilege(s) are given access to the resources.

3 TOE Security Environment

The TOE security environment consists of the organizational security policies and usage assumptions as they relate to TOE. The TOE provides for a level of protection that is appropriate for IT environments that require control over what information is accessed by the users on the systems. It is suitable for use in both commercial and government environments. The organizational security policies enforced by the TOE are sufficient to mitigate and counter any implied threat to the assets protected by the TOE.

3.1 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to TOE and its environment.

P.OBJ_ACCESS	The TOE must limit the access to, modification of, and destruction of the resource objects to those users that are authorized to access to the resource object.
P.ACCOUNTABILITY	Users of the system shall be held accountable for their security relevant actions within the system.
P.AUTH_USERS	Only those users who have been authorized to access the information within the TOE may access the TOE.
P.MANAGE	The TOE must provide authorized administrators with utilities to effectively manage the security-related functions of the system.
P.TRANSIT	The TOE must have the ability to protect system data during transmission between distributed parts of the TOE.

3.2 Secure Usage Assumptions

This section describes the security aspects of the environment in which the TOE will be utilized. This includes information about the physical, personnel, and system aspects of the environment.

3.2.1 Physical Assumptions

A.PROTECT	The components of TOE software critical to security policy enforcement must be located within controlled access facilities that will protect the TOE components from unauthorized physical access and modification.

3.2.2 Personal Assumptions

A.AUTH_DATA	Authorized users of the TOE will keep all their authentication data private.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The administrative personnel are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the administrative guidance.
A.TRAINED_STAFF	Authorized TOE users and administrators are trusted to follow the guidance provided for the secure operation of the TOE

3.2.3 System Assumptions

A.OS	It is assumed that the operating system has been configured in accordance with the manufacturer's installation guides and where applicable, in its evaluated configuration. It is securely configured such that the operating system protects the TOE from any unauthorised users or processes.
A.SYSTEM	The underlying environment will provide protection to the TOE and its related data and a reliable system time.

4 Security Objectives

This section describes the security for the TOE and its supporting environment. Security objectives, categorized as either security objectives of the TOE or security objectives of the environment, reflect the stated intent to enforce the organizational security policies and address assumptions.

4.1 Security Objectives of the TOE

The following security objectives are intended to be satisfied by the TOE and its security related functions.

O.ACCOUNTABILITY	The TSF must records the security relevant actions of the users of the TOE to ensure that users are held accountable for their actions on the TOE.
O.AUTHORIZE	The TSF must ensure that only authorized users and administrators gain access to the TOE and its resources.
O.MANAGE	The TSF must 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.OBJ_ACCESS	The TSF must limit access to objects maintained by the TOE to users with authorization and appropriate privileges. The TSF must allow authorized users to specify which users may access their objects and the actions performed on the objects.
O.TRANSFER	The TSF must have the capability to protect TSF data in transmission between distributed parts of the TOE

4.2 Security Objective of the IT Environment

The following security objectives for the IT environment of the TOE must be satisfied in order for the TOE to fulfill its own security objectives.

OE.AUDITING	The IT environment must ensure that the audit records are available and provides the authorized user with the means to review the audit record.
OE.AUTHORIZED	The IT environment must ensure that TOE administrative users are authenticated before access to the TOE and its resources is granted
OE.SEP	The TOE operating environment shall provide mechanisms to isolate the TSF and assure that TSF components cannot be tampered with or bypassed.
OE.TIME	The operating environment shall provide an accurate timestamp.

4.3 Security Objective of the Non - IT Environment

The following security objectives are intended to be satisfied by the environment of the TOE.

OE.CREDEN	Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users in a manner that maintains IT security objectives.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE and its operating environment is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives.
OE.PERSON	Authorized users of the TOE shall be properly trained in the configuration and usage of the TOE and are trusted to follow the guidance provided for secure operation.
OE.PHYCAL	Those responsible for the TOE must ensure that the parts of the TOE critical to security policy are protected from physical attack that might compromise the TOE security objectives.

5 IT Security Requirements

This section of the ST details the security functional requirements (SFR) for the TOE and the IT Environment that will support the TOE. The SFR were drawn from the CC Part 2.

The following table lists the security functional requirements of the TOE and the IT environment.

Security Functional Class	Security Functional Requirements
TOE Requirements	
Security Audit (FAU)	FAU_GEN.1 Audit Data Generation
	FAU_GEN.2 User Identity Association
User Data Protection (FDP)	FDP_ACC.2 Complete Access Control
	FDP_ACF.1 Security attribute based access control
Identification and Authentication (FIA)	FIA_AFL.1 Authentication failure handling
	FIA_ATD.1 User Attribute Definition
	FIA_UAU.2 User authentication before any action
	FIA_UID.2 User identification before any action
Security management (FMT)	FMT_MOF.1 Management of security functions behaviour
	FMT_MSA.1 Management of Security Attributes
	FMT_MSA.3 Static attribute initialization
	FMT_MTD.1 Management of TSF data
	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security roles
Protection of the TSF (FPT)	FPT_ITT.1 Basic internal TSF data transfer protection
	FPT_RVM.1 Non-bypassability of the TSP
IT Environment	
Security Audit (FAU)	FAU_SAR.1 Audit Review
	FAU_SAR.3 Selectable Audit Review
	FAU_STG.1 Protected audit trail storage
	FAU_STG.4 Prevention of audit data loss
Protection of the TSF (FPT)	FPT_SEP.1 TSF domain separation
	FPT_STM.1 Reliable time stamps

Table 1: Security Functional Requirements

5.1 TOE Security Functional Requirements

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1 Audit data generation

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

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

b) All auditable events for the [***not specified***] level of audit***;*** and

c) [**All modification to the user security attributes including the authentication data**

d) **All modification to the objects' security attributes**

e) **All modification to the behavior of the TSF**

f) **All attempts to access objects.**

g) **All attempts to log into the TOE.**].

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, [**item type**].

5.1.1.2 FAU_GEN.2 User identity association

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 FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the [**Access Control SFP**] on [**subject: all users and objects: resources**] and all operations among subjects and objects covered by the SFP.

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

5.1.2.2 FDP_ACF.1 Security attribute based access control

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

Subject: User

- **The user identity and group membership(s)**
- **Privileges/Privilege sets**

Objects: Resource

- **ACL**

].[i]

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

If the subject has the privilege, object access is granted if at least one of the following conditions is true:

- **If Public Access is enable and ACL explicitly grants requested access to the public, or**
- **ACL explicitly grants requested access to the subject, or**
- **ACL denies access to the public, does not define a subject rule and ACL explicit grants access to the subject's group,**

].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**the subject has superuser access privilege**].

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

5.1.3 Identification and Authentication (FIA)

5.1.3.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [**an administrator configurable setting[0 - 32767]**] unsuccessful authentication attempts occur related to [**user logon**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**lock the user account, and ensures it remains locked until unlocked by an authorized administrator**].

5.1.3.2 FIA_ATD.1 User attribute definition

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

a) **user identity,**

b) **group identity/membership,**

c) **authentication data,**

d) **privileges**

].

5.1.3.3 FIA_UAU.2 User authentication before any action

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

[i] The requirement complies with International Interpretation #103

user.

5.1.3.4 FIA_UID.2 User identification before any action

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 FMT_MOF.1 Management of security functions behaviour (Audit)

FMT_MOF.1.1 The TSF shall restrict the ability to [***modify the behaviour of***] the functions [**audit**] to [**authorized administrator**].

5.1.4.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [**Access Control SFP**] to restrict the ability to [***change_default, query, modify, delete,*** **create**] the security attributes [**user identity, group membership, privileges**] to [**authorized administrator**].

5.1.4.3 FMT_MSA.3 Static attribute initialization

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

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

5.1.4.4 FMT_MTD.1(a) Management of TSF data (Login Attempts Threshold)

FMT_MTD.1.1 The TSF shall restrict the ability to [***modify***] the [**unsuccessful login attempts threshold**] to [**authorized administrator**].

5.1.4.5 FMT_MTD.1(b) Management of TSF data (Authentication Data)

FMT_MTD.1.1 The TSF shall restrict the ability to [***change_default, modify,*** **initialize**] the [**authentication data of non-administrative users**] to [**authorized administrator**].

5.1.4.6 FMT_MTD.1(c) Management of TSF data (Authentication Data)

FMT_MTD.1.1 The TSF shall restrict the ability to [***modify***] the [**their own authentication data**] to [**authorized non-administrative user**].

5.1.4.7 FMT_MTD.1(d) Management of TSF data (Access Control List(ACL))

FMT_MTD.1.1 The TSF shall restrict the ability to [***change_default, modify***] the [**ACL**] to [**authorized administrator**].

5.1.4.8 FMT_SMF.1 Specification of Management Functions[ii]

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

a) **Management of user attributes; which includes the ability to create, modify, delete, and unlock user accounts**,

b) **Management of object security attributes,**

c) **Ability to configure the unsuccessful login attempts threshold,**

d) **Ability to determine the events that will be logged in the event tables**

].

5.1.4.9 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [**authorized administrator, authorized non-administrative 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 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from [***disclosure, modification***] when it is transmitted between separate parts of the TOE.

5.1.5.2 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2 IT Environment Security Functional Requirements

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [**authorized administrator, non-administrative users**] with the capability to read [**all records allowed by user privilege**] from the audit records.

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

5.2.1.2 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform [***searches, sorting***] of audit data based on [**user identity, item type**].

[ii] This requirement has been added to comply with International Interpretation #65

5.2.1.3 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [***prevent***] **unauthorized** modifications to the audit records **in the audit trail**.[iii]

5.2.1.4 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [***prevent auditable events, except those taken by the authorized user with special rights***] and [**take no other action**] if the audit trail is full.

5.2.2 Identification and Authentication

5.2.2.1 FIA_UAU.2 User authentication before any action

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

5.2.3 Protection of the TSF (FPT)

5.2.3.1 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.2.3.2 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

[iii] The requirement has been modified to comply with International Interpretation #141

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the components included in Evaluation Assurance Level (EAL) 3augmented with ALC_FLR.1 as specified in Part 3 of Common Criteria.

Assurance Class	Assurance Components
Class ACM: Configuration management	ACM_CAP.3 Authorization Controls
	ACM_SCP.1 TOE CM Coverage
Class ADO: Delivery and operation	ADO_DEL.1 Delivery Procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.2 Security-enforcing high-level design
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ALC: Life-cycle Support	ALC_DVS.1 Identification of security measures
	ALC_FLR.1 Basic flaw remediation
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: High-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Class AVA: Vulnerability assessment	AVA_MSU.1 Examination of guidance
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

Table 2: Assurance Components for EAL3

5.3.1 Class ACM: Configuration Management

5.3.1.1 ACM_CAP.3 Authorisation Controls

ACM_CAP.3.1D The developer shall provide a reference for the TOE.

ACM_CAP.3.2D The developer shall use a CM system.

ACM_CAP.3.3D The developer shall provide CM documentation.

ACM_CAP.3.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.3.2C	The TOE shall be labeled with its reference.
ACM_CAP.3.3C	The CM documentation shall include a configuration list and a CM plan.
International Interpretation RI #3	**The configuration list shall uniquely identify all configuration items that comprise the TOE.**[iv]
ACM_CAP.3.4C	The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.3.5C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.3.6C	The CM system shall uniquely identify all configuration items.
ACM_CAP.3.7C	The CM plan shall describe how the CM system is used.
ACM_CAP.3.8C	The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.3.9C	The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.3.10C	The CM system shall provide measures such that only authorised changes are made to the configuration items.
ACM_CAP.3.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 ACM_SCP.1 TOE CM Coverage

ACM_SCP.1.1D	The developer shall provide **a list of configuration items for the TOE**.[v]
ACM_SCP.1.1C	**The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST**.[vi]
~~ACM_SCP.1.2C~~	~~The CM documentation shall describe how configuration items are tracked by the CM system~~.[vii]
ACM_SCP.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Class ADO: Delivery and Operation

5.3.2.1 ADO_DEL.1 - Delivery procedures

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.

[iv] This requirement has been added to comply with International Interpretation #3
[v] This requirement has been modification to conform with Interpretation RI #4
[vi] This requirement has been modification to conform with Interpretation RI #4
[vii] This requirement has been deleted to conform with Interpretation RI #4

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

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.[viii]
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 Class ADV: Development

5.3.3.1 ADV_FSP.1 Informal functional specification

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 ADV_HLD.2 Security enforcing high-level design

ADV_HLD.2.1D	The developer shall provide the high-level design of the TSF.
ADV_HLD.2.1C	The presentation of the high-level design shall be informal.
ADV_HLD.2.2C	The high-level design shall be internally consistent.
ADV_HLD.2.3C	The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.2.4C	The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.2.5C	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.2.6C	The high-level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.2.7C	The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

[viii] This requirement has been modified to comply with International Interpretation #51.

ADV_HLD.2.8C	The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.
ADV_HLD.2.9C	The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.
ADV_HLD.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_HLD.2.2E	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 ADV_RCR.1 Informal correspondence demonstration

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 Class AGD: Guidance Documents

5.3.4.1 AGD_ADM.1Administrator guidance

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 AGD_USR.1 User guidance

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 Class ALC: Life-cycle Support

5.3.5.1 ALC_DVS.1 Identification of security measures

ALC_DVS.1.1D	The developer shall produce development security documentation.
ALC_DVS.1.1C	The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.1.2C	The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.
ALC_DVS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_DVS.1.2E	The evaluator shall confirm that the security measures are being applied.

5.3.5.2 ALC_FLR.1 Basic flaw remediation

ALC_FLR.1.1D	The developer shall provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.1.1C	The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.1.2C	The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.1.3C	The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.1.4C	The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE

users.

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

5.3.6 Class ATE: Tests

5.3.6.1 ATE_COV.2 Analysis of coverage

ATE_COV.2.1D	The developer shall provide an analysis of the test coverage.
ATE_COV.2.1C	The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.2.2C	The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.
ATE_COV.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.2 ATE_DPT.1 Testing: high-level design

ATE_DPT.1.1D	The developer shall provide the analysis of the depth of testing.
ATE_DPT.1.1C	The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.
ATE_DPT.1.2E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence

5.3.6.3 ATE_FUN.1 Functional testing

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.

5.3.6.4 ATE_IND.2 Independent testing – sample

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.

5.3.7 Class AVA: Vulnerability Assessment

5.3.7.1 AVA_MSU.1 Examination of guidance

AVA_MSU.1.1D	The developer shall provide guidance documentation.
AVA_MSU.1.1C	The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AVA_MSU.1.2C	The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.1.3C	The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.1.4C	The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).
AVA_MSU.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_MSU.1.2E	The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.
AVA_MSU.1.3E	The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.3.7.2 AVA_SOF.1 Strength of TOE security function evaluation

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.

5.3.7.3 AVA_VLA.1 - Developer vulnerability analysis

AVA_VLA.1.1D The developer shall perform **a vulnerability analysis**[ix]

AVA_VLA.1.2D The developer shall **provide vulnerability analysis documentation**[x]

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.**[xi]

AVA_VLA.1.2C **The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.**[xii]

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**[xiii]

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.

[ix] This requirement has been modified to comply with International Interpretation #51.
[x] This requirement has been modified to comply with International Interpretation #51.
[xi] This requirement has been modified to comply with International Interpretation #51
[xii] This requirement has been modified to comply with International Interpretation #51.
[xiii] This requirement has been added to comply with International Interpretation #51.

6 TOE Summary Specification

6.1 TOE Security Functions

Each of the security function descriptions is organized by the security requirements corresponding to the security function. Hence, each function is described based on how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions are suitable to satisfy the necessary requirements.

6.1.1 Audit Function

TOE logged the security-related and non-security related actions of the users. There is no specific shutdown or startup command that is invoked as auditing is enabled at installation and continuously runs until the system, database, and libraries are stopped.

The security-related events that are audited are as follows:

- All modification to the user security attributes including the authentication data.
- All modification to the resources' security attributes.
- All modification to the behavior of the TSF.
- All attempts to access resources.
- All attempts to log into the TOE.

Each event log entry contains the following information: date and time the event occurred, event code (event type), and identity of the user that performed the action that triggered the generation of the entry. The type of event log generated and the contents of the log define the outcome of the action. (FAU_GEN.1, FAU_GEN.2)

The events are logged in event tables that are stored on and protected by the embedded database located in the IT Environment. The database prevents any modification or deletions to the event tables that were not authorized by an authorized administrator. The events administrative-related and logon actions are stored in the event table, ICMSTSYSADMEVENTS and events related to the resources are stored in ICMSTITEVENTS. Only the authorized administrator has the capability to the delete event logs when the event tables reach their maximum capacity. The database prevents any other auditable events from occurring, with the exception of those caused by the actions of the authorized administrator with the appropriate privilege, reducing the number of event log lost.

An authorized user with the appropriate privilege is able to review the event log history of resources that they have been granted access. The authorized administrator is able to review, search and sort by the user identity and the item type all event logs. The event log is presented in a readable and understandable format.

The Audit function demonstrates the implementation of the following security functional requirements:

- FAU_GEN.1
- FAU_GEN.2

6.1.2 Identification and Authentication

The users and the administrators of Content Manager are able to access the TOE via the use of user ID and password. (FIA_UAU.2, FIA_UID.2)

The non-administrative users of Content Manager are identified and authenticated against user's information stored in the user definition table of the Library Server. The administrative users are authenticated by the underlying operating environment, and then identified against the user ID stored in the

Library Server. Once the users are successfully identified and authenticated, access to the TOE and its resources is granted.

Each user account includes a counter that tracks the number of unsuccessful attempts to authenticate into the Contact Manager. When the administrator-configured number of allowed attempts is exceeded, the TOE locks the user account until the authorized administrator unlocks the account by resetting the counter to zero. (FIA_AFL.1)

The user definition is stored in a table on the Library Server. The information consists of the user identity, group identity, assigned privilege sets, authentication data (password) and the unsuccessful authentication counter. (FIA_ATD.1)

The password associated with each non-administrative users meet the following password policies:

- Passwords must be at least six (6) characters
- Each password must contain at least two alphabetic characters and at least one numeric or special character. The valid characters are upper and lowercase alphabetic characters, 10 numeric characters and the following special characters: !, @, #, $, %, ^, &, *, (,).
- The password should not use consecutive sequences, dictionary words, or easily guessable.
- Each password must differ from the user's user ID and any reverse or circular shift of that user ID.
- New passwords must differ from the old by at least three characters.

The Identification and Authentication function demonstrates the implementation of the following security functional requirements:

- FIA_AFL.1
- FIA_ATD.1
- FIA_UAU.2
- FIA_UID.2

6.1.3 User Data Protection

The Content Manager implements an access control policy based on the privileges/privilege sets, resources, user id and user groups, and ACLs.

Each user is assigned a privilege set which defines the actions that the user can perform on a resource if the ACL grants the actions.

The ACL is associated with each resource managed by Content Manager. The ACL consists of users, groups and the privileges that are associated with each user and group. The ACL defines rules that restrict the actions an user is allowed to perform on a resource. The ACL defines three types of rules; Public, User, and Group, (listed in order of precedence from highest to lowest.). The Public rule authorizes all users based on the ACL assigned actions. The User rule defines the actions granted to individual users. And the Group Rule defines the action(s) granted a group.

When the user initiates an action on a resource, the policy first verifies the user’s privilege(s), and then the ACL to determine if the user has the right to perform the initiated action.

If the user has the required privilege(s), the policy then begins the process of checking that the ACL allows the action:

- First the process verifies that Public Access has been enable. If Public Access has been enable, the process checks the Public rule. If the privilege(s) assigned to the public allow the action, the check is successful, and the access is granted.

- If check fails, or Public Access is disable, the process will check against the User rule. If the rule for the user that initiated the action does not grant the user that specified action, access will be denied, else access is granted.
- However if the ACL does not define a rule for the user, then the process continues to check against the Group rule.

  If the user is part of the group and has the required privileges, then access is granted, else it is denied and the process stops.
- If a user assigned the superuser access privilege (ItemSuperAccess), then the process bypasses the ACL checks and access is granted. (FDP_ACC.2, FDP_ACF.1)

The User Data Protection function demonstrates the implementation of the security functional requirements: FDP_ACC.2 and FDP_ACF.1.

6.1.4 Security Management

Content Manager includes a specific group named sysadmin_group, which specifies the name of the system group that has administrative authority to TOE.

The Content Manager also defines the non-administrative users that are assigned privileges by the authorized administrator to access the resources managed by the Resource Manager. (FMT_SMR.1)

Content Manager restricts the administrative functions to the authorized administrator with appropriate privileges. The System Administration Client provides the interface utilized by the authorized administrator to perform the administrative functions. (FMT_SMF.1) The functions include the ability to select which group of administrative events and the type of item events that will be logged in the event tables, modify the unsuccessful login attempts threshold, the ability to unlock the user accounts, change_default, and modify the restricted values of the ACL associated to an resource, the ability to change_default, query, modify, delete, and create user security attributes, with the exception of the password, The authorized administrator has the ability to initialize, configure, modify and change the default password and current password for any non-administrative user. (FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1(a), FMT_MTD.1(b), FMT_MTD.1(d))

The authorized non-administrative user is able to change their own password. (FMT_MTD.1(c))

The default ACL associated to resources is configured by the authorized administrators and access is restricted based on the rules defined. If there are no rule defined, then access is denied to all users with the exception of the authorized administrator.

The Security Management function demonstrates the implementation of the following security functional requirements:

- FMT_MOF.1
- FMT_MSA.1
- FMT_MSA.3
- FMT_MTD.1(a)
- FMT_MTD.1(b)
- FMT_MTD.1(c)
- FMT_MTD.1(d)
- FMT_SMF.1

6.1.5 Protection of the TSF

The Content Manager employs three different mechanisms to transmit TSF data between components. The mechanisms are one-way hashing, and a security token. The two mechanisms ensure that the TSF data is protected from disclosure and modification when transmitted between TOE components.

The Content Manager does a one-way hash when transmitting passwords between separate parts of the TOE. The algorithm of one-way hashing is Base 64 encoding which does not require a key. The access control data is transmitted as part of a security token.

The Content Manager utilizes a resource security token to ensure that the access control information is protected from disclosure and modification when transmitted to the Resource Manager where the resource requested is stored. The security token contains the resource item ID, version ID, action to be performed and a timestamp for when the access granted will expire. Upon receipt of the token by the Resource manager, the Resource Manager will perform a validation of the token, any attempts modify the security token will cause the validation to fail, and the action will be denied. (FPT_ITT.1)

Access to the administrative functions by the administrator and to resources by users is only possible if the user and administrator have been successfully identified and authenticated. The access to resources is further limited to the privileges that are assigned to the users and the ACL assigned to the resource. Access is only granted when the user has been authorized by the resource's ACL. Once access is granted, a resource security token is sent to the Resource Manager, which will validate the token and allow access if the token has not been modified or expired. (FPT_RVM.1)

The Protection of the TSF function demonstrates the implementation of the FPT_ITT.1 and FPT_RVM.1.

6.2 Security Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL3 augmented with ALC_FLR.1 assurance requirements:

- Process Assurance;
- Delivery and Guidance;
- Design Documentation;
- Tests; and
- Vulnerability Assessment.

6.2.1 Process Assurance

6.2.1.1 Configuration Management

The configuration management measures applied by IBM ensure that configuration items are uniquely identified, and that the procedures documented in the configuration management documentation are used to control and track changes to the CM items. IBM ensures changes to the configuration item are properly controlled. The configuration items under CM control are the TOE implementation representation, design documentation, tests, user and administrator guidance, lifecycle documentation, vulnerability assessment, and the CM documentation:

- IBM DB2 Content Manager for Multiplatforms v8.2 Configuration Management, Issue 1.0, 12 February 2004

The configuration management documentation satisfies:

- ACM_CAP.3
- ACM_SCP.1

6.2.1.2 Life Cycle Support

The lifecycle documentation describes the adequacy of the procedures used during the development and maintenance of the TOE through the use of a comprehensive life-cycle management plan.

The documentation describes the physical, procedural, personnel, and other development security measures that are used in the development environment to protect the TOE. It includes the physical security of the development location and any procedures used to select development staff. It further describes the procedures utilized to track all reported security flaws, the status on correcting the flaw and what measures are to be taken to correct the flaw.

- IBM DB2 Content Manager for Multiplatform v8.2 Lifecycle document, IBM, SVL-Process-0238/lc, Issue 1.1, 12 Feb 2004
- IBM DB2 Content Manager for Multiplatform v8.2 Flaw Remediation, IBM, SVL-Process-0283/fr, Issue 1.3, 12 May 2004

This measure satisfies the following requirements:

- ALC_DVS.1
- ALC_FLR.1

6.2.2 Delivery and Guidance

6.2.2.1 Delivery and Installation

IBM provides documentation that explains how the TOE is delivered, the carriers utilized and the procedures that are able to maintain security when distributed. IBM's installation procedures describe the steps used for the secure installation, generation, and start-up of the TOE along with configuration settings to secure the TOE privileges and functions.

The delivery process is documented in the IBM Delivery Operations and the installation, start-up and generation procedures are documented in:

- IBM DB2 Content Manager for Multiplatforms v8.2, Delivery, Operation, and Guidance, Issue 1.1, 12 March 2004;
- IBM Content Manager for Multiplatforms Planning and Installing Your Content Management System, Version 8, Release 2, October 2003

The delivery and installation documentation satisfies the following assurance requirements:

- ADO_DEL.1,
- ADO_IGS.1.

6.2.2.2 Administrative and User Guidance

IBM provides administrator guidance on how to utilize the TOE security functions, and warnings to authorized administrators about actions that can compromise the security of the TOE. The procedures included in the administrator guidance describe the steps necessary to operate TOE in accordance with the evaluated configuration, detailing how to establish and maintain the secure configuration.

The user guidance describes the procedures to use the TOE security-related functions that are available to the non-administrative users. The procedures describe how to utilize the functions and the associated interfaces in the evaluated configuration.

The administrator guidance is documented in:

- IBM Content Manager for Multiplatforms System Administration Guide, Version 8, Release 2, October 2003
- Online helps files for the Administrator

The user guidance is documented in:

- Online help file for the Client for Windows,

The guidance documentation satisfies the following assurance requirements:

- AGD_ADM.1,
- AGD_USR.1.

6.2.3 Design Documentation

IBM provides design documentation that includes a description of the aspects of the TOE security design, architecture and interfaces. The design documentation consists of the following:

- Functional Specification – details the interfaces and the functions of the TOE.
- High-Level Design – provides a high level description of the TOE, its security functions in terms of subsystems, and describes the interfaces that communicate between the subsystems.
- Representation Correspondence – provides a mapping of the security functions and requirements to the descriptions provide in the design documentation.

The design is described in:

- IBM DB2 Content Manager for Multiplatforms Version 8.2 Security High-level Functional Specification And Design, IBM, SVL-SPEC-0614/fs, Issue 2.0, 16 Mar 2004

The design documentation satisfies the following security assurance requirement:

- ADV_FSP.1;
- ADV_HLD.2; and,
- ADV_RCR.1.

6.2.4 Tests

The Content Manager's test documentation has been created to demonstrate appropriate breadth and depth of coverage. The test documentation describes how all security relevant functions are tested. The test documentation includes test cases and variations necessary to demonstrate that all security checks and effects related to the interfaces are correctly implemented. The test documentation provides correspondence between the security-relevant interfaces and applicable tests and test variations. The test documentation describes the procedures to successfully execute the tests, and expected results of the tests. The test documentation also includes results in the form of logs resulting from completely exercising all of the security test procedures.

The test documentation consists of the following:

- IBM DB2 Content Manager for Multiplatforms v8.2 Security Related Test Cases, Issue 1.4, 4 June 2004
- Design Document Mapping Document, v3.

The test documentation satisfies the following assurance requirements:

- ATE_COV.2;
- ATE_DPT.1
- ATE_FUN.1; and,
- ATE_IND.2.

6.2.5 Vulnerability Assessment

The administrator guidance documentation describes the operation of the TOE and how to maintain a secure state. The administrator guide also describes all operating assumptions and security requirements outside the scope of control of the TOE. The administrator guidance documentation has been developed to serve as a complete, clear, consistent, and reasonable administrator reference.

The strength of TOE security function analysis demonstrates that the SOF claims made in the ST for all probabilistic or permutation mechanisms are correct. IBM performs vulnerability analyses of the TOE to

identify weaknesses that can be exploited in the TOE. IBM documents the status of identified vulnerabilities and demonstrates that for each vulnerability the vulnerability cannot be exploited in the intended environment and that the TOE is resistant to obvious penetration attacks.

- IBM DB2 Content Manager for Multiplatforms Version 8.2 Vulnerability Analysis, Issue 1.3, 01 June 2004

The vulnerability analysis documentation satisfies the following assurance requirements:

- AVA_MSU.1;
- AVA_SOF.1; and,
- AVA_VLA.1.

7 Protection Profile Claims

This TOE does not claim conformance to a Protection Profile.

8 Rationale

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

- Security Objectives;
- Security Requirements;
- Security Functional Requirement Dependencies;
- TOE Summary Specification;
- Strength of Function; and
- Internal Consistency.

8.1 Security Objectives Rationale

This section demonstrates that secure usage assumptions and organizational security policies are completely covered by security objectives. Each objective addresses or enforces at least one assumption, or organizational security policy.

Objectives	O.OBJ_ACCESS	O.ACCOUNTABILITY	O.AUTHORIZE	O.MANAGE	O.TRANSFER	OE.AUDITING	OE.AUTHORIZED	OE.SEP	OE.TIME	OE.CREDEN	OE.INSTALL	OE.PERSON	OE.PHYSAL
A.AUTH_DATA										X			
A.MANAGE										X		X	
A.NOEVIL												X	
A.OS								X			X		X
A.PROTECT											X		X
A.SYSTEM								X	X				X
A.TRAINED_STAFF												X	
P.OBJ_ACCESS	X			X									
P.ACCOUNTABILITY		X		X		X			X				
P.AUTH_USERS			X				X			X			
P.MANAGE			X	X			X						
P.TRANSIT					X								

Table 3: Policies, and Assumptions vs. Security Objectives

8.1.1 Security Objectives for the TOE

This section describes how the Security Objectives for the TOE and the Environment completely and effectively enforce the organizational policies.

O.OBJ_ACCESS — This objective ensures that the TSF controls access to the objects and the actions performed on the objects managed by the TOE thus supporting the

	enforcement of P.OBJ_ACCESS.
O.ACCOUNTABILITY	This objective ensures that the TOE monitors, and audits the security-related actions of the users and administrators, thus supporting the enforcement of P.ACCOUNTABILITY.
O.AUTHORIZE	This objective ensures that only authorized users have access to the TOE, its functions, and the objects the TOE manages. This objective enforces P.AUTH_USERS, and supports the enforcement of P.MANAGE.
O.MANAGE	This objective ensures that the TOE provides the tools necessary for the authorized administrator to manage the security-related functions; audit function, access control function, and other administrative functions, supporting the enforcement of P.OBJ_ACCESS, P.ACCOUNTABILITY, and P.MANAGE.
O.TRANSFER	This objective ensures that the TSF data is protected from disclosures and modification as it is transmitted between the distributed components of the TOE, thus enforcing P.TRANSIT.

8.1.2 Security Objectives for the Environment

This section demonstrates how the IT environment security objectives are effect in addressing the assumptions made about the operating environment, personnel and the physical location of the TOE.

8.1.2.1 Security Objectives for the IT Environment

OE.AUDITING	This objective ensures that the environment provides the tools required to store, and view the audit records, supporting the enforcement of P.ACCOUNTABILITY.
OE.AUTHORIZED	This objective ensures that the environment authenticates that TOE administrative users before access is granted. This supports the enforcement of P.MANAGE, and P.AUTH_USERS
OE.SEP	This objective provides the support needed by the TOE to assisting in addressing A.SYSTEM and A.OS by ensuring that the TOE and it associated data cannot be tampered with or bypassed.
OE.TIME	This objective ensures that an accurate timestamp is provided for the TOE use to accurately record information on a time/date basis, supporting A.SYSTEM and the enforcement of P.ACCOUNTABILITY.

8.1.2.2 Security Objectives for the Non-IT Environment

OE.CREDEN	This objective ensures that users of the TOE keep their authentication data (password) private. This objective supports A.AUTH_DATA, A.MANAGE and the enforcement of P.AUTH_USERS.
OE.INSTALL	This objective ensures that the TOE and its operating environment is installed, configured, managed and administered in a secure manner by a competent and security aware individual in accordance with the administrator, delivery and installation documentation for the TOE and the operating environment. This objective supports A.PROTECT and A.OS.
OE.PERSON	This objective ensures that the TOE is managed and administered in a secure manner by competent and security aware personnel in accordance with the administrator documentation. Thus, supporting A.NOEVIL, A.MANAGE,

	and A.TRAINED_STAFF
OE.PHYCAL	This objective ensures that the TOE is operated in an environment that will protect it from unauthorized access and physical threats and attacks that can disturb and corrupt the data generated and protected by the TOE. This objective addresses A.PROTECT, A.OS, and A.SYSTEM.

8.2 Security Requirements Rationale

This section demonstrates the internal consistency and completeness of the security requirements included in this Security Target. Table 4: Security Functional Requirements vs. Security Objectives indicates the requirements that effectively satisfy each individual objective. Objectives for the IT environment are satisfied only by requirements for the IT environment; however some of those requirements also support, indirectly, the TOE security 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.

Objectives / Functional Requirements	O.OBJ_ACCESS	O.ACCOUNTABILITY	O.AUTHORIZE	O.MANAGE	O.TRANSFER	OE.AUDITING	OE.AUTHORIZED	OE.SEP	OE.TIME
FAU_GEN.1		X							
FAU_GEN.2		X							
FAU_SAR.1						X			
FAU_SAR.3						X			
FAU_STG.1						X			
FAU_STG.4						X			
FDP_ACC.2	X								
FDP_ACF.1	X								
FIA_AFL.1			X						
FIA_ATD.1	X		X						
FIA_UAU.2			X				X		
FIA_UID.2			X						
FMT_MOF.1				X					
FMT_MSA.1	X		X	X					
FMT_MSA.3	X			X					
FMT_MTD.1(a)			X	X					
FMT_MTD.1(b)			X	X					
FMT_MTD.1(c)			X						
FMT_MTD.1(d)	X								

Objectives / Functional Requirements	O.OBJ_ACCESS	O.ACCOUNTABILITY	O.AUTHORIZE	O.MANAGE	O.TRANSFER	OE.AUDITING	OE.AUTHORIZED	OE.SEP	OE.TIME
FMT_SMF.1				X					
FMT_SMR.1			X						
FPT_ITT.1					X				
FPT_RVM.1	X								
FPT_SEP.1								X	
FPT_STM.1									X

Table 4: Security Functional Requirements vs. Security Objectives

The following text describes how each security objective is satisfied by the SFRs:

O.ACCOUNTABILITY *The TSF must records the security relevant actions of the users of the TOE to ensure that users are held accountable for their actions on the TOE.*

FAU_GEN.1 and FAU_GEN.2 define the security-related events that are auditable, the contents of the audit records and ensures that the user that caused the event is identified in the event logged.

The abovementioned requirements ensure the generation of audit records, that the audit records are associated to the user that caused the event.

O.AUTHORIZE *The TSF must ensure that only authorized users and administrators gain access to the TOE and its resources.*

FIA_UAU.2 and FIA_UID.2 ensure that the TOE provides an identification and authentication mechanism to authorize the users that access to the TOE and its associated data.

FIA_AFL.1, FMT_MTD.1(a), and FMT_MTD.1(b), ensures that the TOE locks out a user who makes a number of unsuccessful attempts to logon, that the authorized administrator has the ability to set the number unsuccessful login attempts, the management of the authentication data, and the ability to unlock user accounts.

FIA_ATD.1, FMT_MSA.1 and FMT_MTD.1(b) define the user identification and authentication data, and privileges and restrict the management of the user attributes to the authorized administrator.

FMT_MTD.1(c) ensures that the authorized non-administrative user has the ability to modify their own authentication data.

FMT_SMR.1 defines the roles that must be maintained by the TOE. These roles are the authorized administrators and authorized non-administrative users of the TOE.

These requirements work together to ensure that only authorized users have access to the TOE and the data the TOE is managing.

O.MANAGE *The TSF must allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are*

able to access such functionality.

FMT_MOF.1 ensures that the ability to manage the audit function is restricted to the authorized administrator.

FMT_MSA.1, FMT_MSA.3, and FMT_MTD.1(b) ensure that the management of the user's security attributes is restricted to the authorized administrator.

FMT_MTD.1(a) ensures that the ability to modify the unsuccessful login attempts threshold is restricted to the authorized administrator.

FMT_SMF.1 ensures the authorized administrator is provided the capability to change and maintain security relevant data and functions.

These requirements work together to ensure that the security functions are restricted to the authorized administrator and the administrator has the capability to management the TSF and the associated TSF data.

O.OBJ_ACCESS	*The TSF must limit access to objects maintained by the TOE to users with authorization and appropriate privileges. The TSF must allow authorized users to specify which users may access their objects and the actions performed on the objects.*

FDP_ACC.2 and FDP_ACF.1 define the access control SFP that TOE use to grant users access to the objects managed by the TOE.

FIA_ATD.1 defines the security attributes that are associated to the user and used by the SFP.

FMT_MSA.1 and FMT_MSA.3 restrict the ability to change_default, query, modify, create, and delete security attributes to authorized administrators, ensures that restrictive default values are defined for the security attributes used to enforce the SFP.

FMT_MTD.1(d) restricts the ability to change_default and modify the object's ACL to the authorized administrator.

FPT_RVM.1 ensures that the access control SFP is enforced with each request for access to an object managed by the TOE.

These requirements work together to ensure the enforcement of the SFP policies, limiting access to objects and ensuring that the ability to manage the security attributes used by the SFP is restricted to the authorized user.

O.TRANSFER	*The TSF must have the capability to protect TSF data in transmission between distributed parts of the TOE*

FPT_ITT.1 ensures that the TSF data is not disclosed or modified when transmitted between the components of the TOE.

This requirement ensures that the TSF data is protected when transmitted between the components of the TOE.

OE.AUDITING	*The IT environment must ensure that the audit records are available and provides the authorized user with the means to review the audit record.*

FAU_SAR.1, FAU_SAR.3, ensure that the IT Environment provides the records in a readable format and capability to review, search and sort the audit records by the authorized user.

FAU_STG.1 and FAU_STG.4 ensures that the audit records are available for review by ensuring that the audit records are protected from unauthorized deletions and limit the amount of audit records lost when the audit logs are full.

The abovementioned requirements ensure that the audit records are protected and available for review by the authorized user.

OE.AUTHORIZED	*The IT environment must ensure that TOE administrative users are authenticated before access to the TOE and its resources is granted*

FIA_UAU.2 ensures that the IT Environment authenticates the TOE administrative users before access to the TOE is granted.

The requirement ensures that the TOE, and its resources are only accessible to authorized administrators for the TOE.

OE.SEP	*The TOE operating environment shall provide mechanisms to isolate the TSF and assure that TSF components cannot be tampered with or bypassed.*

FPT_SEP.1 ensures that the IT Environment protects the TOE and it resources from external tampering.

The requirement ensures that the environment protects the TOE from untrusted process that could attempt to tamper with or bypass the TOE.

OE.TIME	*The operating environment shall provide an accurate timestamp.*

FPT_STM.1 ensures that the environment provides accurate and reliable time mechanism, which may be utilized by the TOE.

This requirement ensures that the environment has a timing mechanism which accurate and reliable.

8.2.2 Security Functional Requirement Dependency Rationale

The dependencies of the TOE security functional requirements are met through the functionality of the TOE and/or by the security functionality of the IT environment.

Table 5: Security Functional Requirements Dependencies maps the TOE security functional requirements to the corresponding requirements they are dependent on, demonstrating that all TOE security functional requirement dependencies are met within the ST.

Note: the table below assumes the requirement iterations have the same dependencies and therefore the iterations are not individually identified in the table (e.g. FMT_MTD.1(a)).

Dependency / Functional Requirements	FAU_GEN.1	FAU_SAR.1	FAU_STG.1	FDP_ACC.2	FDP_ACF.1	FIA_UAU.2	FIA_UID.2	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1
FAU_GEN.1													X
FAU_GEN.2	X						X						
FAU_SAR.1	X												
FAU_SAR.3		X											
FAU_STG.1	X												
FAU_STG.4			X										
FDP_ACC.2					X								

Dependency / Functional Requirements	FAU_GEN.1	FAU_SAR.1	FAU_STG.1	FDP_ACC.2	FDP_ACF.1	FIA_UAU.2	FIA_UID.2	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1
FDP_ACF.1				X					X				
FIA_AFL.1						X							
FIA_UAU.2							X						
FMT_MOF.1											X	X	
FMT_MSA.1				X							X	X	
FMT_MSA.3								X				X	
FMT_MTD.1											X	X	
FMT_SMR.1							X						

Table 5: Security Functional Requirements Dependencies

Note: FIA_AFL.1 has a dependency on FIA_UAU.1 and FIA_UAU.2 has a dependency on FIA_UID.1. These dependencies are met with FIA_UAU.2 and FIA_UID.2 respectively (which are hierarchical to the indicated requirements).

8.2.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL3 augmented assurance package. The EAL chosen is based on the statement of the security environment (assumptions, and organizational policy) and the security objectives defined in this ST. The augmentation was chosen to provide the added assurance acquired by defining flaw remediation procedures and correcting security flaws. The sufficiency of the EAL chosen (EAL3) is justified based on those aspects of the environment that have impact upon the assurance needed in the TOE. The administrative staff is conscientious, non-hostile and well trained (A.NOEVIL, A.MANAGE, and OE.PERSON) and all users of the TOE protect all access control data (i.e. password) (OE.CREDEN). The TOE is physically protected (OE.PHYCAL), and properly and securely configured (OE.INSTALL). Given these aspects, a TOE based on good commercial development and maintenance practices is sufficient. EAL3 augmented is an appropriate level of assurance for the TOE described in this ST.

8.3 TOE Summary Specification Rationale

This section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions and security assurance measures are suitable to meet the TOE security requirements and that the collection of security functions work together to provide all of the security requirements. Table 6: Security Functional Requirements vs. Security Functions demonstrates that functions described are sufficient to substantiate the SFRs.

Table 7: Security Assurance Requirements vs. Assurance Measures provides a mapping of TOE security assurance functions to those security assurance measures that have been implemented by the developer to ensure that the TOE meets the requirements specified by CC EAL3 augmented with ALC_FLR.1.

Security Functions / Functional Requirements	AUDIT	IDENTIFICATION AND AUTHENTICATION	USER DATA PROTECTION	SECURITY MANAGMENT	PROTECTION OF THE TSF
FAU_GEN.1	X				
FAU_GEN.2	X				
FDP_ACC.2			X		
FDP_ACF.1			X		
FIA_AFL.1		X			
FIA_ATD.1		X			
FIA_UAU.2		X			
FIA_UID.2		X			
FMT_MOF.1				X	
FMT_MSA.1				X	
FMT_MSA.3				X	
FMT_MTD.1(a)				X	
FMT_MTD.1(b)				X	
FMT_MTD.1(c)				X	
FMT_MTD.1(d)				X	
FMT_SMF.1				X	
FMT_SMR.1				X	
FPT_ITT.1					X
FPT_RVM.1					X

Table 6: Security Functional Requirements vs. Security Functions

Assurance Measures / Assurance Requirements	PROCESS ASSURANCE	DELIVERY AND GUIDANCE	DEVELOPMENT	TESTS	VULNERABILITY ASSESSMENT
ACM_CAP.3	X				
ACM_SCP.1	X				
ADO_DEL.1		X			
ADO_IGS.1		X			
ADV_FSP.1			X		
ADV_HLD.2			X		
ADV_RCR.1			X		

Assurance Measures / Assurance Requirements	PROCESS ASSURANCE	DELIVERY AND GUIDANCE	DEVELOPMENT	TESTS	VULNERABILITY ASSESSMENT
AGD_ADM.1		X			
AGD_USR.1		X			
ALC_DVS.1	X				
ALC_FLR.1	X				
ATE_COV.2				X	
ATE_DPT.1				X	
ATE_FUN.1				X	
ATE_IND.2				X	
AVA_MSU.1					X
AVA_SOF.1					X
AVA_VLA.1					X

Table 7: Security Assurance Requirements vs. Assurance Measures

8.4 Strength of Function Rationale

The TOE minimum strength of function of SOF-basic was chosen to be consistent with the TOE. A SOF-claim is associated with the authentication mechanism described in Identification and Authentication which supports FIA_UAU.2 and the one-way hashing described in Protection of TSF which supports FPT_ITT.1.

The SOF-basic strength level is sufficient to meet the objectives of the TOE, O.AUTHORIZED, given the organizational policies the TOE and its environment must enforce, specifically P.AUTH_USERS, and P.MANAGE and O.TRANSIT which ensures that information transited is secure.

8.5 Internal Consistency and Support

The selected functional requirements for the TOE and IT Environment are internally consistent. All the operations performed are in accordance with the CC. The ST does not include any instances of a requirement that conflicts with or contradicts another requirement. In instances where multiple requirements apply to the same function, the requirements and their operations do not cause a conflict between each other.

The selected requirements are mutually supportive by supporting the dependencies as demonstrated in Table 5, the rationale of the suitability of the requirements to meet the objectives; the inclusion of architectural requirements, FPT_RVM.1 and FPT_SEP.1, to protect the TOE; the inclusion of audit requirements to detect security-related actions and the inclusion of management requirements to provide a means to properly configure and manage the other security requirements.

References

Common Criteria for Information Technology Security Evaluation Part 1, CCIMB-99-031, Version 2.1, August 1999.

Common Criteria for Information Technology Security Evaluation Part 2, CCIMB-99-032, Version 2.1, August 1999.

Common Criteria for Information Technology Security Evaluation Part 3, CCIMB-99-033, Version 2.1, August 1999.