Risk Management System 3.2.06.12
Security Target

Version 1.0
June 26, 2006

DOCUMENT INTRODUCTION

Prepared By:

COACT, Inc.
9140 Guilford Road, Suite L
Columbia, Maryland 21046-2587

Prepared For:

SecureInfo Corporation
211 North Loop 1604 East
Suite 200
San Antonio, TX 78232

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the SecureInfo Risk Management System (RMS) Version 3.2.06.12 Security Target. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Figures

List of Tables

ACRONYMS LIST

CC ..... Common Criteria
EAL2 ..... Evaluation Assurance Level 2
I&A ..... Identification and Authentication
IT ..... Information Technology
NIAP ..... National Information Assurance Partnership
PP ..... Protection Profile
SF ..... Security Function
SFP ..... Security Function Policy
SFR ..... Security Functional Requirement
SOF ..... Strength of Function
ST ..... Security Target
TOE ..... Target of Evaluation
TSC ..... TSF Scope of Control
TSF ..... TOE Security Functions
TSFI ..... TSF Interface
TSP ..... TOE Security Policy

CHAPTER 1

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the SecureInfo Risk Management System (RMS) Version 3.2.06.12. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.2*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9* and all National Information Assurance Partnership (NIAP) and International Interpretations through February 2, 2005. As such, the spelling of terms is presented using internationally accepted English.

1.1 Security Target Reference

This section provides identifying information for the SecureInfo Risk Management System (RMS) Version 3.2.06.12 Security Target by defining the Target of Evaluation (TOE).

1.2 Security Target Name

SecureInfo Risk Management System (RMS) Version 3.2.06.12 Security Target.

1.2.1 TOE Reference

SecureInfo Risk Management System (RMS) Version 3.2.06.12

1.2.2 Security Target Evaluation Status

This ST is currently under evaluation.

1.2.3 Evaluation Assurance Level

Functional and assurance claims conform to EAL2 (Evaluation Assurance Level 2) from the *Common Criteria for Information Technology Security Evaluation, Version 2.2*.

1.2.4 Keywords

Keywords – Common Criteria (CC), Security Target (ST), Evaluation Assurance Level 2 (EAL2), Security Function (SF), Security Function Policy (SFP), Target of Evaluation (TOE), TOE Security Functions (TSF), TOE Security Policy (TSP).

1.3 TOE Overview

This Security Target defines the requirements for the SecureInfo Risk Management System (RMS) Version 3.2.06.12. RMS is the Target of Evaluation (TOE). RMS is a software tool that generates security Certification and Accreditation (C&A) document templates that a customer can tailor to become compliant with government and other regulatory mandates. The TOE logical boundary is described in Chapter 2 along with the evaluated configuration of the TOE.

1.3.1 Security Target Organization

Chapter 1 of this ST provides introductory and identifying information for the TOE.

Chapter 2 describes the TOE and provides some guidance on its use.

Chapter 3 provides a security environment description in terms of assumptions, threats and organizational security policies.

Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) Environment.

Chapter 5 provides the TOE security and functional requirements, as well as requirements on the IT Environment.

Chapter 6 is the TOE Summary Specification, a description of the functions provided by the SecureInfo Risk Management System (RMS) Version 3.2.06.12 to satisfy the security functional and assurance requirements.

Chapter 7 identifies claims of conformance to a registered Protection Profile (PP).

Chapter 8 provides a rationale for the security objectives, requirements, TOE summary specification and PP claims.

1.4 Common Criteria Conformance

The SecureInfo Risk Management System (RMS) Version 3.2.06.12 Security Target is compliant with the *Common Criteria for Information Technology Security Evaluation, Version 2.2*, functional requirements (Part 2) conformant, assurance requirements (Part 3) conformant for EAL2.

1.5 Protection Profile Conformance

The SecureInfo Risk Management System (RMS) Version 3.2.06.12 does not claim conformance to any registered Protection Profile.

CHAPTER 2

2. TOE Description

This section provides the context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 SecureInfo Risk Management System (RMS) Version 3.2.06.12 TOE Description

This section provides a description of the SecureInfo Risk Management System (RMS) Version 3.2.06.12 TOE. RMS is a software tool that generates security Certification and Accreditation (C&A) document templates that a customer can tailor to become compliant with government and other regulatory mandates. It provides a formal network C&A process to determine the level-of-risk and maintain overall security posture of an organization's enterprise information infrastructure. This process allows end users to comply with all federal and corporate regulations, using a proven methodology to ensure that a required combination of security measures are implemented in order to address and measure relevant risk and vulnerability. Using RMS, a user develops all required security documentation necessary to perform a complete C&A.

Using RMS, organizations can develop the security documentation needed to comply with a variety of US Federal certification and corporate regulatory compliance processes (DITSCAP, NIACAP, FISMA), including:

A) Detailed Outlines and Templates

B) Specialized Instructions

C) Working Examples

D) Documentation Creation and Maintenance

E) Consistent Compliance Deliverables

As regulations change, C&A-compliant documents are made available to customers.

Access to RMS is a simple client/server relationship using the Internet Explorer web browser on the client system. The client is not part of the TOE and is outside the scope of this evaluation.

Due to the potential sensitivity of the information contained, RMS was developed to limit accessibility to those with a need-to-know. Therefore, RMS supports identification and authentication, access control, and role management features. These features limit access to RMS, RMS data elements, and support three roles: RMS system administrator, domain manager, and user.

2.2 SecureInfo Risk Management System (RMS) Version 3.2.06.12 Physical and Logical Boundaries

This section describes the physical and logical boundaries of the SecureInfo Risk Management System (RMS) Version 3.2.06.12 TOE.

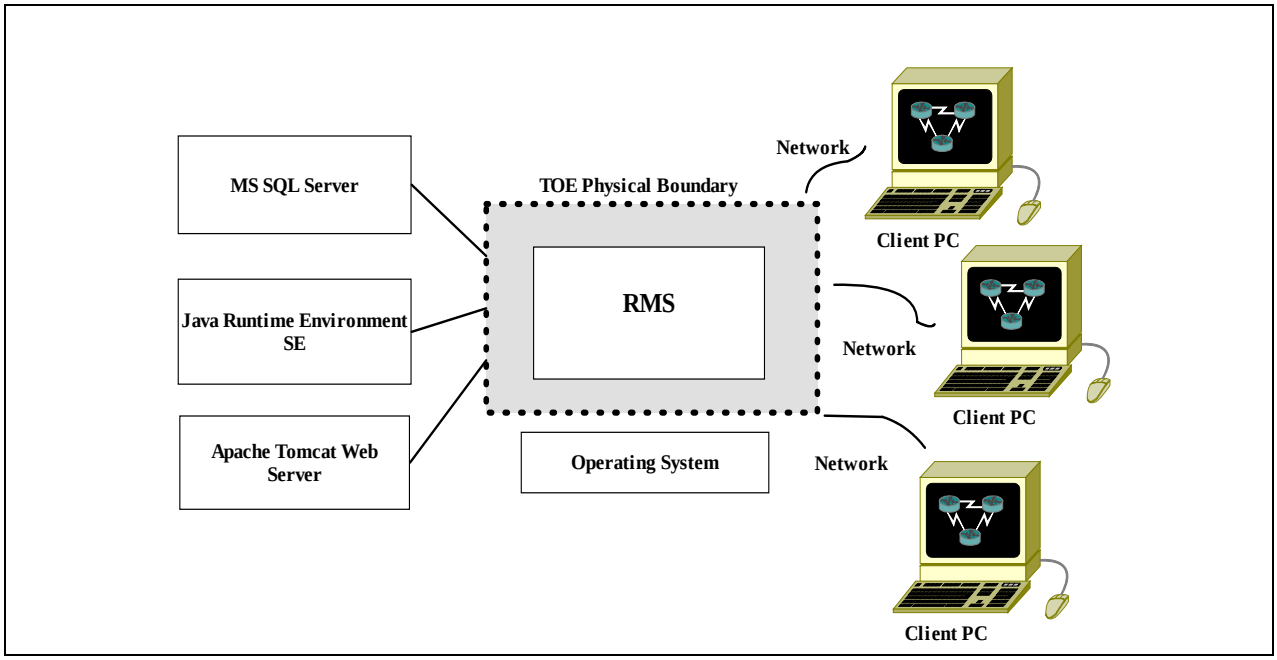
2.2.1 Physical Boundary

This section provides context for the TOE evaluation by describing the physical boundaries of the TOE. The TOE is the SecureInfo Risk Management System (RMS) Version 3.2.06.12

product. The TOE runs on a Windows 2000 operating system and relies on the operating system and the hardware in the IT Environment for operation. The operating system and hardware are addressed by the IT Environment descriptions. The operating system and hardware are included by inference and are not part of the TOE.

The RMS TOE physical boundaries are depicted in Figure 1. Those items that are out of the scope of evaluation are the underlying operating system and hardware, MS SQL 2000, Java Runtime Environment SE and Apache Tomcat Web Server.

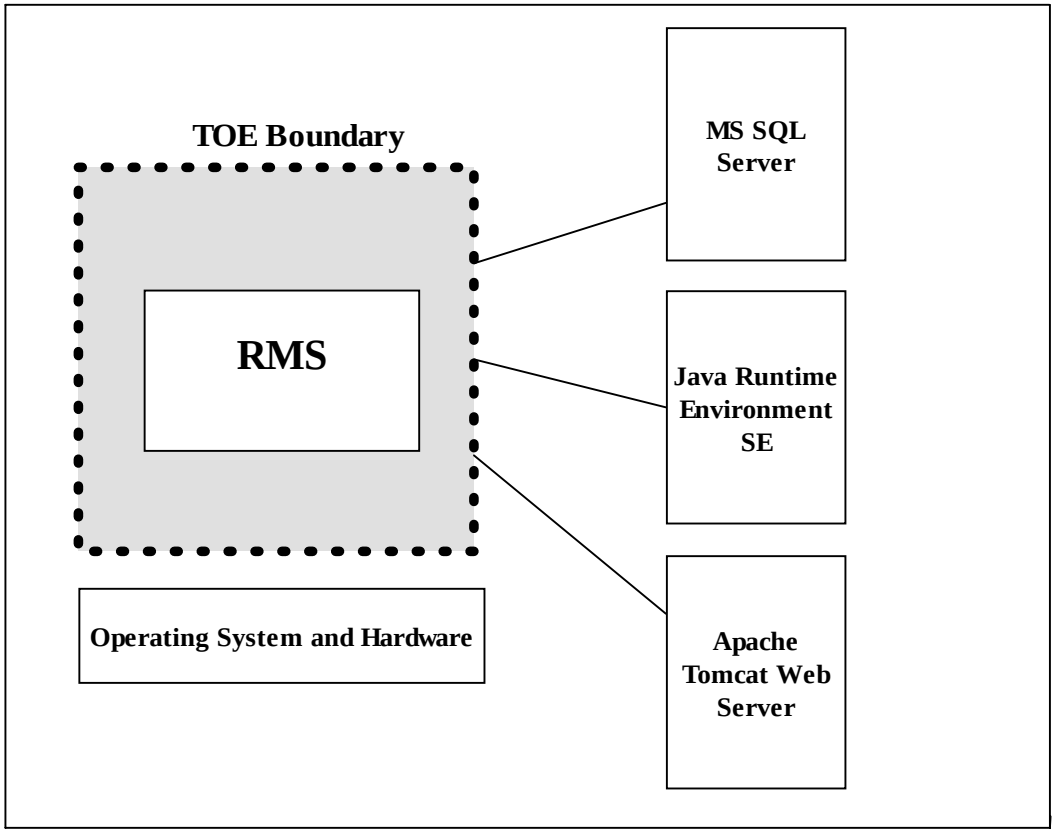
Figure 1 - RMS TOE Physical Boundary



2.2.2 Logical Boundary

This section provides context for the TOE evaluation by describing the logical boundaries of the TOE. The TOE is the SecureInfo Risk Management System (RMS) Version 3.2.06.12 product. The TOE runs on a Windows 2000 operating system and relies on the operating system and the hardware in the IT Environment for operation. The operating system and hardware are addressed by the IT Environment descriptions. The operating system and hardware are included by inference and are not part of the TOE. The RMS logical boundaries are depicted in Figure 2. The rectangle represented by the dash lines indicates the RMS TOE logical boundary.

Figure 2 - RMS TOE Logical Boundary



The RMS logical TOE boundaries are defined by the security functions provided by the TOE and are described in the following sections.

A) Identification and Authentication (I&A): The TOE requires users to identify and authenticate themselves before accessing the TOE, and therefore, by default, before viewing any TSF data or configuring any portion of the TOE. No action can be initiated before proper identification and authentication. Each TOE user has security attributes associated with their account that defines the functionality the user is allowed to perform.

B) Access Control: The TOE uses access control to address security attribute usage and characteristics of policies and may have the ability to explicitly authorize or deny access to an object based upon security attributes. Specifically, security attribute-based access control allows the TOE to enforce access based upon security attributes and named groups of attributes.

C) Role Management: The TOE supports three security roles: Authorized RMS System Administrator, Domain Manager, and Authorized User. These roles are defined within the TOE. An authorized RMS System Administrator has the ability to define groups and other roles to assist in the management of access rights and privileges. A Domain Manager has full access to and has the ability to create user accounts in his or her domain. Authorized Users are users that are authorized to use some TOE resources.

2.3 SecureInfo Risk Management System (RMS) Version 3.2.06.12 Evaluated Configuration

The evaluated configuration of the TOE is depicted in Figure 1 - RMS TOE Boundary above. The parameters of the TOE that are outside the scope of evaluation are the underlying operating system and associated hardware, MS SQL Server 2000, Java Runtime Environment SE and Apache Tomcat Web Server. The Operational Environment is addressed in Table 1 and 2 below. It should be noted that the Client hardware/software is outside the scope of this evaluation.

2.3.1 Operational Environment

The evaluated configuration will follow the password guidance as stated in the RMS administrative guidance and as detailed below:

A) Passwords must be a minimum length of eight characters and include at least one alphabetic character, one numeric character, and one special character.

B) Passwords shall not be reusable by the same user identifier.

C) The TSF shall not indicate to the user if he/she has chosen a password already associated with another user.

D) The TSF shall, by default, prohibit the use of null passwords during normal operation.

The following tables specify the hardware and software required for the operation of the TOE.

Table 1 - Client Hardware/Software Requirements

Hardware	Software
Intel platform or compatible Intel Pentium 3 800 MHz or higher 256 MB RAM 1 GB Hard Drive Network connection	MS Windows 2000 (all editions) MS Internet Explorer 6.0 or higher

Table 2 - Database Server Hardware/Software Requirements

Hardware	Software
Intel platform or compatible Intel Pentium 4 2.0 GHz or higher 1 GB RAM 40 GB Hard Drive Network connection	MS Windows 2000 Server or Windows 2003 Server with current Service Packs and Hot fixes MS Internet Explorer 6.0 or higher Sun Java 2 SE SDK 1.4.2_04 MS SQL Server 2000 SP3a Apache Tomcat 4.1.30 MS SQL Server 2000 Driver for JDBC SP2, The driver must be installed in the <Tomcat base>\ common\ lib folder.

CHAPTER 3

3. TOE Security Environment

This chapter identifies Assumptions (AE), Threats Addressed by the TOE (T), and Threats to be Addressed by the Operating Environment (TE) related to the TOE. Assumptions detail the expected environment and operating conditions of the system. Threats are those that are addressed by the TOE and operating environment.

3.1 Assumptions

The assumptions are ordered into three groups. They are physical assumptions, personnel assumptions, and IT environment assumptions.

A) Personnel assumptions describe characteristics of personnel who are relevant to the system.
B) Physical environment assumptions describe characteristics of the non-IT environment that the system is deployed in.
C) IT environment assumptions describe the technology environment within which the TOE is operating.

3.1.1 Physical Assumptions

AE.LOCATE	The processing resources of the TOE will be located within controlled access facilities that will prevent unauthorized physical access.

3.1.2 Personnel Assumptions

3.1.3 IT Environment Assumptions

AE.CONNECT	Any other systems with which the TOE directly and interactively communicates is under the management control of the organization in which the system is deployed and operates under the same security policy constraints as the TOE.
AE.PROTECT	The hardware and software critical to the execution of the TOE will be protected from unauthorized access.
AE.JUSTAPPS	Applications executing on the RMS server are limited to the TOE and applications that the TOE is dependent on for proper and secure execution. No other application will be installed, generated, or executed on the RMS server.

3.2 Threats

The threats identified in the following subsections are addressed by the TOE and IT environment, respectively.

3.2.1 Threats Addressed by the TOE

T.ACCESS	An unauthorized individual may attempt to gain access to the TOE, a TOE resource, or to information directly controlled by the TOE, via user error, system error, or an unsophisticated, technical attack.

T.NOAUTH	An authorized user may attempt to access information specific to the RMS System Administrator, Domain Manager or another user that is stored by the TOE by circumventing the access control function.

3.2.2 Threats Addressed by the Operating Environment

TE.ACCESS	An unauthorized individual may gain access to information not protected by the TOE in the operating environment, including TOE data stored outside the TOE.

3.3 Organizational Security Policies

There are no Organizational Security Policies identified for this TOE.

CHAPTER 4

4. Security Objectives

4.1 Security Objectives for the TOE

O.ACCESS	The TOE identifies and authenticates users prior to allowing access to TOE functions and resources.
O.IDAUTHORIZE	The TOE provides access by authenticated users to those TOE resources and actions for which they have been authorized. The TOE must provide the ability to specify and manage user access rights to individual data elements under its control.

4.2 Security Objectives for the Operating Environment

OE.ACCESS	The TOE physical and operating environment must guard against unauthorized access to information not protected by the TOE in the operating environment, including TOE data stored outside the TOE.

4.3 Rationale for Security Objectives for the TOE

This section provides the rationale that all security objectives are traced back to aspects of the addressed threats.

O.ACCESS - O.ACCESS addresses T.ACCESS because the TOE identifies and authenticates users prior to allowing access to TOE functions and resources and protects unauthorized access to information by unauthorized individuals through either malicious or accidental means.

O.IDAUTHORIZE - O.IDAUTHORIZE addresses T.NOAUTH because the TOE must ensure that all users are identified and authenticated before being granted access to the TOE mediated resources. The TOE provides the ability to specify and manage user access rights to the RMS System Administrator and Domain Manager.

4.4 Rationale for Security Objectives for the Operating Environment

This section provides the rationale that all security objectives are traced back to aspects of the addressed assumptions and threats.

OE.ACCESS - OE.ACCESS addresses TE.ACCESS by ensuring that the operating environment protects against unauthorized access to information not protected by the TOE in the operating environment, including TOE data stored outside the TOE.

OE.ACCESS - OE.ACCESS addresses AE.LOCATE by ensuring that physical access controls are in place to prevent unauthorized access to the TOE.

OE.ACCESS - OE.ACCESS addresses AE.CONNECT by ensuring that TOE users with physical access to the TOE have the privileges necessary to access the connected networks and operate the TOE in a secure manner.

OE.ACCESS - OE.ACCESS addresses AE.PROTECT by ensuring that the hardware and software critical to the execution of the TOE will be protected from unauthorized access and physical modification of information not protected by the TOE in the operating environment, including TOE data stored outside the TOE.

OE.ACCESS - OE.ACCESS addresses AE.JUSTAPPS by ensuring that TOE users with physical access to the TOE have the privileges necessary to access the applications executing on the RMS server and that these privileges are limited to the TOE and applications that the TOE is dependent on for proper and secure execution.

ST Author's Note: *The TOE is a software tool executing on its own server. It is assumed the TOE will be housed and managed in a similar manner with other servers. Commonly servers are managed in protected environments usually referred to as 'server farms'. While the RMS System Administrator is responsible for the management and secure operation of the TOE, non-users of the TOE may manage the operating system, the database, and perhaps other applications required by the TOE. In addition, because the TOE is attached to a computer network environment, non-users of the TOE will be responsible for the secure management of systems providing the computer network.*

Table 3 - Mappings Between Threats and Security Objectives for the TOE

Threat/Objective	T.ACCESS	T.NOAUTH
O.ACCESS	X	
O.IDAUTHORIZE		X

Table 4 - Mappings Between Threats, Assumptions, and Security Objectives for the Environment

Threat/Assumption/ Security Objective	TE.ACCESS	AE.LOCATE	AE.CONNECT	AE.PROTECT	AE.JUSTAPPS
OE.ACCESS	X	X	X	X	X

CHAPTER 5

5. IT Security Requirements

This section contains the security requirements that are satisfied by the TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC. The following table summarizes the security functional requirements claimed for the TOE and the IT Environment.

5.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.2* with the exception of the items within the functional requirements identified as operations that are TOE specific.

The CC defines four operations on security functional requirements. The font conventions listed below identify the conventions for the operations defined by the CC.

A) Assignment: indicated in italics

B) Selection: indicated in underlined text

C) Assignments within selections: indicated in italics and underlined text

D) Refinement: indicated with **bold** text

Table 3 identifies the functional requirements that are provided by the TOE and the IT Environment.

Table 5 - Security Functional Requirements (SFRs)

SFR Component	SFR Name
TOE SFRs Derived Verbatim from Part 2 of the CC	
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Security Attribute Based Access Control
FIA_SOS.1	Verification of Secrets
FIA_UAU.2	User Authentication Before any Action
FIA_UAU.7	Protected Authentication Feedback
FIA_UID.2	User Identification before any Action
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

5.2 IT Security Requirements

This section contains the security requirements that are satisfied by the TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC. The following table summarizes the security functional requirements claimed for the TOE and the IT Environment.

5.3 TOE Security Functional Requirements

The TOE security functional requirements for this Security Target consist of the following components from Part 2 of the CC.

5.3.1 User Data Protection (FDP)

5.3.1.1 FDP_ACC.1 Subset Access Control

5.3.1.2 Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the *Access Control Security Function Policy (SFP)* on

A) Subjects – users

B) Objects – Object types as specified in the table below.

C) Operations – Operations are specific to the object type, as specified in the following table:

Object Type	*Add*	*Attach*	*Configure*	*Copy*	*Create*	*Delete*	*Display*	*Edit*	*Execute*	*Move*	*Read*	*Set Project Default*	*Show/Hide*	*View*	*View at Domain Level*	*View at Enterprise Level*	*View at Package Level*	*View at User Level*
Audit Log															*X*	*X*		
Bundle					*X*	*X*		*X*		*X*								
Content Library (Execute RMS)									*X*									
Deprecated Content													*X*					
Enterprise Administration Module							*X*											
Image	*X*					*X*		*X*		*X*				*X*				
Image Folder					*X*	*X*												
Milestone					*X*	*X*		*X*			*X*							
Milestone Folder					*X*	*X*												

Object Type	*Add*	*Attach*	*Configure*	*Copy*	*Create*	*Delete*	*Display*	*Edit*	*Execute*	*Move*	*Read*	*Set Project Default*	*Show/Hide*	*View*	*View at Domain Level*	*View at Enterprise Level*	*View at Package Level*	*View at User Level*
Passwords			*X*															
Project (C&A Package)				*X*	*X*	*X*		*X*		*X*	*X*							
Project Folder (C&A Package Folder)					*X*	*X*												
Questionnaire					*X*	*X*		*X*		*X*	*X*							
Questionnaire Folder					*X*	*X*												
Regulation					*X*	*X*		*X*		*X*	*X*							
Regulation Folder					*X*	*X*												
Requirement					*X*	*X*		*X*		*X*	*X*							
Requirement Folder					*X*	*X*												
RTF (Attachment)		*X*				*X*					*X*							
RTM View					*X*	*X*		*X*			*X*	*X*						
Standard Template				*X*	*X*	*X*		*X*		*X*	*X*							
Standard Template Folder					*X*	*X*												
Standard Template Sub-Document					*X*	*X*		*X*			*X*							
Test					*X*	*X*		*X*		*X*	*X*							
Test Folder					*X*	*X*												
Utilization Reports															*X*		*X*	*X*

Dependencies: FDP_ACF.1 Security Attribute Based Access Control.

5.3.1.3 FDP_ACF.1 Security Attribute Based Access Control

Hierarchical to: No other components.

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

A) Subjects – Permissions, Domain

B) Objects – none.

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

A) Users may only access objects in their Domain (Enterprise Administrators belong to all Domains)

B) The operation is allowed if the user's permission for the operation being attempted against the specific object type is set.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *None.*

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *None.*

Dependencies: FDP_ACC.1 Subset access control.

FMT_MSA.3 Static attribute initialization.

5.3.2 Identification and Authentication (FIA)

5.3.2.1 FIA_SOS.1 Verification of Secrets

Hierarchical to: No other components.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet *the password policy constraints defined by the following attributes:*

1) Passwords must be a minimum length of eight characters and include at least one alphabetic character, one numeric character, and one special character.

2) Passwords shall not be reusable by the same user identifier.

3) The TSF shall not indicate to the user if he/she has chosen a password already associated with another user.

4) The TSF shall, by default, prohibit the use of null passwords during normal operation.

Dependencies: No dependencies.

5.3.2.2 FIA_UAU.2 User Authentication Before any Action

Hierarchical to: FIA_UAU.1 Timing of Authentication.

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

Dependencies: FIA_UID.1 Timing of Identification.

5.3.2.3 FIA_UAU.7 Protected Authentication Feedback

Hierarchical to: No other components.

FIA_UAU.7.1 The TSF shall provide only *obscured feedback* to the user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of Authentication.

5.3.2.4 FIA_UID.2 User Identification before any Action

Hierarchical to: FIA_UID.1 Timing of identification

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.

Dependencies: No dependencies.

5.3.3 Security Management (FMT)

5.3.3.1 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the *access control SFP* to restrict the ability to change_default, query, modify, delete, *and create* the security attributes: *permissions* to *RMS System Administrator* and *Domain Managers.*

Dependencies: [FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

5.3.3.2 FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

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 *RMS System Administrator and Domain Managers* to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

5.3.3.3 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 (1) The TSF shall restrict the ability to create, query, modify, and delete the *following TSF relevant data:*

a. RMS Group,

b. Permissions for a RMS Group,

c. RMS Client Account from a RMS Group,

d. Permissions for a RMS Client Account,

to the *authorized RMS System Administrator.*

Iteration:

FMT_MTD.1.1 (2) The TSF shall restrict the ability to create, query, modify, and delete **under** *that specific domain the following security-relevant TSF data:*

a. RMS Group,

b. Permission for a RMS Group,

c. RMS Client Account from a RMS Group,

d. Permissions for a RMS Client Account,

to the *authorized Domain Manager.*

Dependencies: FMT_SMF.1 Specification of management functions.

FMT_SMR.1 Security roles.

5.3.3.4 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components

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

a. Management of RMS Groups

b. Management of Permissions for a RMS Group

c. Management of RMS Client Accounts from an RMS Group

d. Management of Permissions for a RMS Client Account

Dependencies: No Dependencies

5.3.3.5 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles:

A. Authorized RMS System Administrators

B. Domain Managers

C. Authorized users

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

Dependencies: FIA_UID.1 Timing of Identification.

5.4 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2. These requirements are summarized in Table 4.

Table 6 - Assurance Requirements

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.2	Configuration Items
Delivery and Operation	ADO_DEL.1	Delivery Procedures
Delivery and Operation	ADO_IGS.1	Installation, Generation, and Start-Up Procedures
Development	ADV_FSP.1	Informal Functional Specification
Development	ADV_HLD.1	Descriptive High-Level Design
Development	ADV_RCR.1	Informal Correspondence Demonstration
Guidance Documents	AGD_ADM.1	Administrator Guidance
Guidance Documents	AGD_USR.1	User Guidance
Tests	ATE_COV.1	Evidence of Coverage
Tests	ATE_FUN.1	Functional Testing
Tests	ATE_IND.2	Independent Testing - Sample
Vulnerability Assessment	AVA_SOF.1	Strength of TOE Security Function Evaluation
Vulnerability Assessment	AVA_VLA.1	Developer Vulnerability Analysis

5.5 Security Requirements for the IT Environment

There are no Security Functional Requirements for the IT Environment.

5.6 Rationale for TOE Security Functions

FDP_ACC.1 Subset Access Control. The Access Control feature supports FDP_ACC.1 by ensuring that access control is enforced on users, files, and operations between users and files.

FDP_ACF.1 Security Attribute Based Access Control. The Access Control feature supports FDP_ACF.1 by ensuring that objects cannot be accessed or modified without the proper authorizations.

FIA_SOS.1 Verification of Secrets. The Identification and Authentication feature supports FIA_SOS.1 by ensuring that the use of a password minimum length of eight characters with at least one alphabetic character, one numeric character, and one special character will make brute force attacks difficult for the assumed threat level of SOF-basic.

FIA_UAU.2 User Authentication Before any Action. The Identification and Authentication feature supports FIA_UAU.2 by ensuring that users are authenticated before accessing TOE security functions.

FIA_UAU.7 Protected Authentication Feedback. The Identification and Authentication feature supports FIA_UAU.7 by ensuring that protected authentication feedback is provided using obscured feedback while authentication is in progress.

FIA_UID.2 User Identification before any Action. The Identification and Authentication feature supports FIA_UAU.7 by ensuring that users are identified before accessing TOE security functions.

FMT_MSA.1 Management of Security Attributes. The Role Management feature supports FMT_MSA.1.1 by enforcing the Access Control SFP to restrict the ability to change_default, query, modify, delete, or create the security attributes of domain access, read, and read-write to RMS System Administrator and Domain Managers.

FMT_MSA.3 Static Attribute Initialization. The Role Management feature supports FMT_MSA.3 by ensuring the enforcement of the security policy is made at initialization and that only authorized roles can modify the initial values.

FMT_MTD.1 Management of TSF data. The Access Control feature and the Role Management feature support FMT_MTD.1 by restricting operations that can be performed on TSF data to the authorized roles.

FMT_SMF.1 Specification of Management Functions. The Role Management feature supports FMT_SMF.1 by describing the security management functions that can be configured by the authorized roles.

FMT_SMR.1 Security Roles. The Role Management feature supports FMT_SMF.1 by ensuring that the security management functions are authorized to the proper roles.

The following table shows the mapping between the Security Functional Requirements and the security functions provided by the TOE.

Table 7 - Mapping of Security Functional Requirements to Security Functions

SFR/Security Function	Identification and Authentication (I&A)	Access Control	Role Management
FDP_ACC.1		X	
FDP_ACF.1		X	
FIA_SOS.1	X		
FIA_UAU.2	X		
FIA_UAU.7	X		
FIA_UID.2	X		
FMT_MSA.1		X	X
FMT_MSA.3		X	X
FMT_MTD.1			X
FMT_SMF.1			X
FMT_SMR.1			X

5.7 SFR to Security Objectives Rationale

This section provides the rationale for the functional requirements and demonstrates how each security objective is enforced by the functional requirements.

FDP_ACC.1 — FDP_ACC.1 supports both O.ACCESS and O.IDAUTHORISE because it ensures that users are identified and authenticated before access is granted and that the security policy between subjects, objects, and operations is enforced**.**

FDP_ACF.1 — FDP_ACF.1 supports O.IDAUTHORISE because it ensures that access and operations to objects is limited to user identity and the operations they are authorized to perform.

FIA_SOS.1 — FIA_SOS.1 supports O.ACCESS by ensuring that the use of a password minimum length of eight characters with at least one alphabetic character, one numeric character, and one special character will make brute force attacks difficult for the assumed threat level of SOF-basic.

FIA_UAU.2	FIA_UAU.2 supports O.ACCESS because it ensures that access to the TOE and access to objects cannot be accomplished before successful user authentication. FIA_UAU.2 supports O.IDAUTHORISE by ensuring that users are authenticated to those TOE resources and actions for which they have been authorized before accessing the security functionality of the TOE.
FIA_UAU.7	FIA_UAU.7 supports O.ACCESS because it ensures that passwords are not visible when being entered.
FIA_UID.2	FIA_UID.2 supports O.ACCESS because it ensures that access to the TOE and access to objects cannot be accomplished before successful user identification. FIA_UID.2 supports O.IDAUTHORISE by ensuring that users are authenticated to those TOE resources and actions for which they have been authorized before accessing the security functionality of the TOE.
FMT_MTD.1	FMT_MTD.1 supports O.ACCESS because it ensures that access to TSF functions are restricted to authorized user roles. FIA_MTD.1 supports O.IDAUTHORISE because it restricts operations on TSF data to the authorized roles.
FMT_MSA.1	FMT_MSA.1 supports O.IDAUTHORISE because it ensures that the TSF enforces the Access Control SFP to restrict the ability to change_default, query, modify, delete, or create the security attributes of domain access, read, and read-write to RMS System Administrator and Domain Managers.
FMT_MSA.3	FMT_MSA.3 supports O.IDAUTHORISE because it allows the authorized role to override default values for security attributes.
FMT_SMF.1	FMT_SMF.1 supports O.ACCESS and O.IDAUTHORIZE because it ensures that the TOE must provide access by authorized users to the specified security management functions.
FMT_SMR.1	FMT_SMR.1 supports O.IDAUTHORIZE because it ensures that the TOE must provide access by Authorized RMS System Administrators, Domain Managers, and Authorized users and be able to associate users with roles.

The following table contains a mapping of the TOE security functional requirements and the security objectives each requirement enforces.

Table 8 - Mappings between Security Functional Requirements and Security Objectives for the TOE

SFR/Security Objective	O.ACCESS	O.IDAUTHORIZE
FDP_ACC.1	X	X
FDP_ACF.1	X	
FIA_SOS.1		X
FIA_UAU.2		X
FIA_UAU.7		X
FIA_UID.2		X
FMT_MSA.1		X
FMT_MSA.3		X
FMT_MTD.1 (all iterations)	X	X
FMT_SMF.1	X	X
FMT_SMR.1		X

5.8 Rationale for IT Security Requirement Dependencies

The following table lists the claimed TOE and IT Environment security requirements and their dependencies.

Table 9 - Security Functional Requirements

Claim	Hierarchical to	Dependencies
FDP_ACC.1	None	FDP_ACF.1
FDP_ACF.1	None	FDP_ACC.1 – FMT_MSA.3
FIA_SOS.1	None	None
FIA_UAU.2	FIA.UAU.1	FIA_UID.1
FIA_UAU.7	None	FIA_UAU.1
FIA_UID.2	FIA_UID.1	None
FMT_MSA.1	None	FDP_ACC.1 or FDP_IFC.1 and FMT_SMF.1 and FMT_SMR.1

FMT_MSA.3	None	FMT.MSA.1 and FMT.SMR.1
FMT_MTD.1	None	FMT_SMF.1 and FMT_SMR.1
FMT_SMF.1	None	None
FMT_SMR.1	None	FIA_UID.1

5.9 Rationale for Security Assurance Requirements of the TOE

The TOE meets the assurance requirements for EAL2. The CC states that EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

The SecureInfo Risk Management System (RMS) is a software tool that generates security Certification and Accreditation (C&A) document templates that a customer can tailor to become compliant with government and other regulatory mandates. It provides a formal network C&A process to determine the level-of-risk and maintain overall security posture of an organization's enterprise information infrastructure.

Recent explanatory discussions with NIAP indicate that no software tool is capable of obtaining more than an EAL2 rating because of the requisite partial evaluation on associated operating systems and hardware.

The RMS Certification and Accreditation (C&A) process is independent of the actual informational content of the information system and owner organization being sampled. Actual content is not present. The TOE consists of a Software Application that is not using dependencies from the associated Operating System or Underlying Hardware. As a result, the TOE can also operate on assets that have a stronger EAL rating providing both logical and physical assurance if needed.

EAL2 was chosen based on the statement of the security environment (assumptions, threats and organizational policy) and the security objectives defined in this ST. EAL2 is, therefore, applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.

EAL2 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behavior. The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain). EAL2 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis, and independent testing based upon more detailed TOE specifications.

5.10 Strength of Function (SOF)

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General model, August 1999, defines “Strength of Function (SOF)” in terms of the minimum efforts assumed necessary to defeat the expected security behavior of a TOE security function.

5.10.1 Strength of Function Claims

The only probabilistic or permutational mechanism in the TOE is the password mechanism used to authenticate all users. The claimed minimum strength of function is SOF-basic. FIA_SOS.1 and FIA_UAU.2 are the only TOE security functional requirements that depend on this permutational function.

5.10.2 Strength of Function Rationale

The claimed minimum strength of function is SOF-basic. All user authentication requirements in FIA_SOS.1 and FIA_UAU.2 contain a permutational function requiring a SOF analysis. SOF-basic is defined in CC Part 1 section 2.3 as: "A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential." The rationale for the chosen level is based on the low attack potential of the threat agents identified in this ST and the strength of the minimum password length. Based on the SOF Analysis below, the SOF-basic strength level is sufficient to meet the objectives of the TOE given the security environment described in the ST.

The SecureInfo RMS installer will set the initial RMS System Administrator password to a minimum length of eight characters and include at least one alphabetic character, one numeric character, and one special character as per SecureInfo recommendations found in the RMS Installation procedures. The RMS System Administrator, following the SecureInfo password recommendation found in the Administrator Guide, will change the password to a minimum length of eight characters and include at least one alphabetic character, one numeric character, and one special character. Following the administrative guidance, the RMS System Administrator will also set up the Domain and User accounts following the same SecureInfo password recommendation. The Domain Manager will use the same guidance as found in the Domain Manager guidance.

5.10.3 SOF Analysis

One second was selected as a conservative length of time required to enter a user id and password into RMS. The password space is calculated as follows:

Numeric characters: n=10

Special characters: x=33

Six character length dictionary words: a=14163

Password length: (n*x*a) = 8 (multiplying the three together gives you the possible combinations of a six character word plus a numeral plus a special character)

Seconds per attempt: s = 1

Average length of successful attack in days =

= (s * (n*x*a)) / (2 assuming attacker only needs half the space * (60 * 60 * 24 seconds per day))

= (1 * (10*33*14163)) / (2 * (60 * 60 * 24))

= 4673790 / 2 (half the space)

= 2336895 / 60 seconds

= 38948 seconds / 60 minutes

= 649 minutes / 24 hours

= 27 days

Using the approach detailed in the CEM Part 2 Annex B, the values for “Identifying Value” and "Exploiting Value" in Table B.3 for each factor were summed. Given the simplicity of a brute force attack, all the values are 0 except for the Exploiting Value for Elapsed Time (5) and Access to TOE (6) for a total of 11. As shown in Table B.4, values between 10 and 17 indicate the mechanism is sufficient for a SOF Rating of ‘Basic’, resistant to an attack potential of ‘Low’.

CHAPTER 6

6. TOE Summary Specification

6.1 TOE Security Functions

TOE Security Functions

This section presents the TOE security functions (TSFs) and a mapping of security functions to security functional requirements. The major functions implemented by the TOE are as follows:

A) Access Control: The TOE uses access control to address security attribute usage and characteristics of policies and may have the ability to explicitly authorize or deny access to an object based upon security attributes. Specifically, security attribute-based access control allows the TOE to enforce access and operations based upon security attributes and named groups of attributes.

B) Identification and Authentication (I&A): The TOE requires users to identify and authenticate themselves before accessing the TOE and, therefore, by default, before viewing any TSF data or configuring any portion of the TOE. No action can be initiated before proper identification and authentication. Each TOE user has security attributes associated with their user account that defines the functionality the user is allowed to perform.

C) Role Management: The TOE supports three security roles: Authorized RMS System Administrator, Domain Manager, and Authorized User. These roles are managed within the TOE. An Authorized RMS System Administrator has the ability to define groups and other roles to assist in the management of access rights and privileges. A Domain Manager has full access to and has the ability to create user accounts in his or her domain. Authorized Users are users that are authorized to use some TOE resources.

6.2 Assurance Measures

The assurance measures provided by the TOE satisfy all of the assurance requirements listed in Chapter 5, Table 4. Table 7 below provides a reference between each TOE assurance requirement and the related vendor documentation that satisfies each requirement.

Table 10 - Assurance Measures

Assurance Component	Documentation Satisfying Component	Rationale
ACM_CAP.2	Configuration Management Plan	Measures Used to Meet Component: ACM_CAP.2 This requirement will be met by documentation describing the Configuration Management system used during the development of the TOE. The Configuration Management Plan describes the CM measures to ensure that the configuration items are uniquely identified and changes are accurately tracked. The documentation describes the processes and procedure followed and automated tools that are utilized in the tracking and monitoring the changes to the CM items and the generation of the TOE.
ADO_DEL.1	Delivery Procedures	Measures Used to Meet Component: ADO_DEL.1 This requirement will be met by documentation describing the delivery of the TOE. This delivery and operations data describes the methods and procedures used to distribute and identify the TOE. The administrative guidance describes the interfaces and procedures that are used by the administrator to operate and administer the TOE.
ADO_IGS.1	Installation, Generation and Start-up Documentation	Measures Used to Meet Component: ADO_IGS.1 This requirement will be met by documentation describing the Installation, Generation and Start-up of the TOE. This documentation describes procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. It provides authorized administrator and user

Assurance Component	Documentation Satisfying Component	Rationale
		guidance on how to perform the TOE security functions. It also provides warnings to authorized administrators and users about actions that can compromise the security of the TOE.
ADV_FSP.1	Functional Specification	Used to Meet Component: ADV_FSP.1 This requirement will be met by the Functional Specification for the TOE supported by the Security Target and Administration Guidance documentation. The Functional Specification provides all TSF interface specifications fully describing all interfaces to the TSF.
ADV_HLD.1	High Level Design Document	Measures Used to Meet Component: ADV_HLD.1 This requirement will be met by the high level design for the TOE supported by the Security Target and Functional Specification.
ADV_RCR.1	Security Target, Functional Specification, and related Design Documentation	Measures Used to Meet Component: ADV_RCR.1 This requirement will be met by the Security Target, Functional Specification, and related Design Documentation for the TOE. The Representation Correspondence requirement is satisfied by providing a mapping of the security functions and requirements to the descriptions provided in the design documentation.
AGD_ADM.1	Administrator Guidance documentation	Measures Used to Meet Component: AGD_ADM.1 This requirement will be met by the Administration Guidance documentation supported by the Security Target; Functional Specification; High-Level Design; and Installation, Generation and Start-up documentation. The Administrative Guidance documentation also describes the interfaces and procedures that are used by the administrator to operate

Assurance Component	Documentation Satisfying Component	Rationale
		and administer the TOE. It documents the security functions and the interfaces that are utilized to configure the functions
AGD_USR.1	User Guidance documentation	Measures Used to Meet Component: AGD_USR.1 The user guidance describes the interfaces and procedures that are used to operate the TOE. This guidance documents the security functions, warnings and the interfaces that are utilized to configure the security functions. It also describes actions that can compromise the security of the TOE. User guidance is documented in the RMS 3.2.06 User Guide.
ATE_COV.1	Security Target, Functional Specification, Test documentation and Test Coverage Analysis.	Measures Used to Meet Component: ATE_COV.1 The TOE test documentation describes how all security relevant APIs are tested, specifically describing all test cases and variations necessary to demonstrate that all security checks and effects related to the API are correctly implemented. The test documentation provides correspondence between the security-relevant APIs and applicable tests and test variations. The test documentation describes the actual tests, 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.
ATE_FUN.1	Security Target, Functional Specification, Test documentation and procedures.	Measures Used to Meet Component: ATE_FUN.1 The TOE test documentation describes the security functions to be tested, how to successfully test all of them, the expected results, and the actual test results after exercising all of the tests.

Assurance Component	Documentation Satisfying Component	Rationale
ATE_IND.2	Developer Test Documentation Evaluation Lab Independent Testing Evaluation Deliverables.	Measures Used to Meet Component: ATE_IND.2 This assurance requirement will be met by the functional and penetration tests performed with their test results and a TOE suitable for testing.
AVA_SOF.1	Strength of Function Analysis and Evaluation Deliverables.	Measures Used to Meet Component: AVA_SOF.1 This assurance requirement will be met by Strength of Function Analysis and evaluation deliverables. The strength of TOE security function analysis demonstrates that the SOF claims made in the ST for all probabilistic or permutation mechanisms are correct. Vulnerability analyses of the TOE are performed to identify weaknesses that can be exploited in the TOE. These analyses document the status of identified vulnerabilities and demonstrate that a given vulnerability cannot be exploited in the intended environment and that the TOE is resistant to obvious penetration attacks.
AVA_VLA.1	Vulnerability Analysis, and Evaluation Deliverables	Measures Used to Meet Component: AVA_VLA.1 This assurance requirement will be met by the Vulnerability Analysis, the other evaluation deliverables and a copy of the TOE suitable for testing. The Vulnerability Analysis will identify the vulnerabilities in the TOE. The analysis provides the status of each identified vulnerability and demonstrates that a given vulnerability cannot be exploited in the intended environment and that the TOE is resistant to obvious penetration attacks. Misuse Analysis shows that the administrative and user guidance completely addresses managing the TOE in a secure configuration.

6.2.1 Rationale for TOE Assurance Requirements

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from Part 3 of the Common Criteria.

CHAPTER 7

7. Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 1, Section 1.4 Protection Profile Conformance.

7.1 Protection Profile Reference

This Security Target does not claim conformance to any registered Protection Profile.

7.2 Protection Profile Refinements

This Security Target does not claim conformance to any registered Protection Profile.

7.3 Protection Profile Additions

This Security Target does not claim conformance to any registered Protection Profile.

7.4 Protection Profile Rationale

This Security Target does not claim conformance to any registered Protection Profile.

CHAPTER 8

8. Rationale

This Security Target does not claim conformance to any Protection Profiles.

8.1 Security Objectives Rationale

Sections 4.3 - 4.4 provide the security objectives rationale.

8.2 Security Requirements Rationale

Section 5.6 provides the security function rationale.

8.3 TOE Summary Specification (TSS) Rationale

Section 6.2 provides the TSS rationale.

8.4 Protection Profile Claims Rationale

This Security Target does not claim conformance to any Protection Profiles