Guidance Software EnCase® Enterprise V6.8

Security Target

Version 1.0
19 November 2008

Prepared for:
Guidance Software, Inc.

215 North Marengo Avenue, Second Floor
Pasadena, CA 91101

Prepared By:
Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

Table of Contents

LIST OF FIGURES

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization.

The TOE is EnCase® Enterprise Version 6.8 provided by Guidance Software, Inc. The TOE is a software application that provides a network-enabled, multi-platform enterprise investigation, and incident response solution.

The Security Target contains the following additional sections:

- Section 2 – Target of Evaluation (TOE) Description

  This section gives an overview of the TOE, describes the TOE in terms of physical and logical boundaries, and states the scope of the TOE.

- Section 3 – TOE Security Environment

  This section details the expectations of the environment, the threats that are countered by the TOE and the environment and the organizational policy that the TOE must fulfill.

- Section 4 – TOE Security Objectives

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

- Section 5 – IT Security Requirements

  This section presents the security functional requirements (SFR) for the TOE and the IT Environment that supports the TOE, and details the assurance requirements for EAL2.

- Section 6 – TOE Summary Specification

  This section describes the security functions represented in the TOE that satisfies the security requirements.

- Section 7 – Protection Profile Claims

  This section presents any protection profile claims.

- Section 8 – Rationale

  This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – Guidance Software EnCase® Enterprise Security Target

ST Version – 1.0

ST Date – 19 November 2008

TOE Identification – Guidance Software EnCase® Enterprise, Version 6.8

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.

  - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.
  - Part 3 Conformant
  - EAL 2

1.3 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the Security Target.

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 placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Terminology and Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CC	Common Criteria
CEM	Common Evaluation Methodology
CCEVS	Common Criteria Evaluation and Validation Scheme
CIRT	Computer incident response teams
EAL	Evaluation Assurance Level
EEE	EnCase Enterprise Edition
GUI	Graphical User Interface
PGP	Pretty Good Protection
PKI	Public Key Infrastructure
PP	Protection Profile
SAFE	Secure Authentication For EnCase
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

Term	Definition
Node	Used to refer to a workstation or server that the TOE Servlet component has been installed.

2. TOE Description

The Target of Evaluation (TOE) is EnCase® Enterprise Version 6.8, developed by Guidance Software, Inc. EnCase Enterprise is an enterprise–wide incident response, security, compliance auditing, and forensic discovery software product.

2.1 TOE Overview

EnCase Enterprise is designed for corporate and government organizations that need the ability to perform internal computer investigations of all types. It establishes an investigative infrastructure that provides network-enabled search, identification, preservation, analysis and reporting of digital evidence on employee computers and file servers for the purposes of internal investigations such as fraud, HR matters and computer incident analysis and response. The solution views data at the binary level, providing the capability to find hidden files such as rootkits and identify zero-day exploits. In addition the software provides the ability to remediate malicious processes, and serves as a platform for add-on data discovery capabilities (not included in the evaluated configuration) for the purposes of sensitive data auditing and eDiscovery.

2.2 TOE Architecture

EnCase Enterprise has three main components that are installed separately. The components that comprise the TOE are the Secure Authentication For EnCase (SAFE), the Examiner, and the Servlet.

SAFE (Secure Authentication For EnCase) **–** The SAFE is the software component that is used to authenticate administrators, administer access rights, retain logs of EnCase Enterprise transactions, broker communications, and provide for secure data transmission. The SAFE communicates with Examiners and targeted Servlets using encrypted data streams, ensuring no information can be intercepted and interpreted.

Examiner – The Examiner is the system used by authorized administrators to perform incident response, investigations, and audits on designated systems. Note a user with access to the Examiner component of the TOE can generate an encryption key pair (for themselves or another user) without being identified or authenticated by the TOE. Additionally, a user with access to the Examiner can attempt to launch an investigation on the local machine on which the Examiner is installed, again without being identified or authenticated by the TOE (although the user needs to have administrative privileges in the underlying Windows OS on the local machine if the investigation is to produce any useful information). This type of investigation is not within the scope of the intended method of use of the product.

Servlet – The Servlet is the agent software that is installed on targeted workstations and servers. The Servlet allows the SAFE and the Examiner to preview, acquire and analyze volatile and static data residing on targeted machines. The Servlets exist passively on these machines as agents, and do not directly implement any security functions. However, the Servlet does support the access control decisions of the SAFE, by only accepting authenticated connections by the SAFE.

Supported platforms and recommended system specifications for these components are listed below.

SAFE	Examiner	Servlet
Supported Platforms		
Windows 2000 Windows XP Windows Server 2003	Windows 2000 Windows XP Windows Server 2003	• Windows – 9X/ME, NT/2K/XP/2003 • Linux – Kernels 2.4 and newer with the Process File System (procfs)

SAFE	Examiner	Servlet
		• Solaris – 8 & 9 (32 and 64-bit) • AIX – 4.3, 5.1, 5.2 & 5.3 (32 and 64-bit) • OS/X – 10.2-10.5 • NetWare – 5.1 SP8, 6.0 SP4 and 6.5
Suggested System Requirements		
Pentium IV or higher 512 MB RAM or higher 15MB free HD or higher	Pentium III or higher 512 MB RAM or higher 15MB free HD or higher	N/A

The following diagrams illustrate the architecture of the TOE and the two types of virtual connections that are used to gather data from the Servlets.

Forensic Concurrent Connections: A secure virtual connection that is established between the Examiner and target machines. The number of concurrent connections controls the number of machines that can potentially be forensically analyzed simultaneously.

One of the capabilities of EnCase Enterprise is the ability to "preview" computers over the network. A preview is the process of securely reaching across the network to a running system or systems that have the Servlet component installed and remotely view all data (unallocated, deleted, allocated, file slack, volume slack, and file system attributes) on hard drives, RAID arrays, CD ROMs, FireWire devices, mounted PGP volumes, and thumb drives in a forensically sound fashion. Conducting a preview does not alert the user nor does it make changes to the machine being investigated. This critical capability enables administrators to quickly determine whether relevant evidence or suspect artifacts exist on a computer.

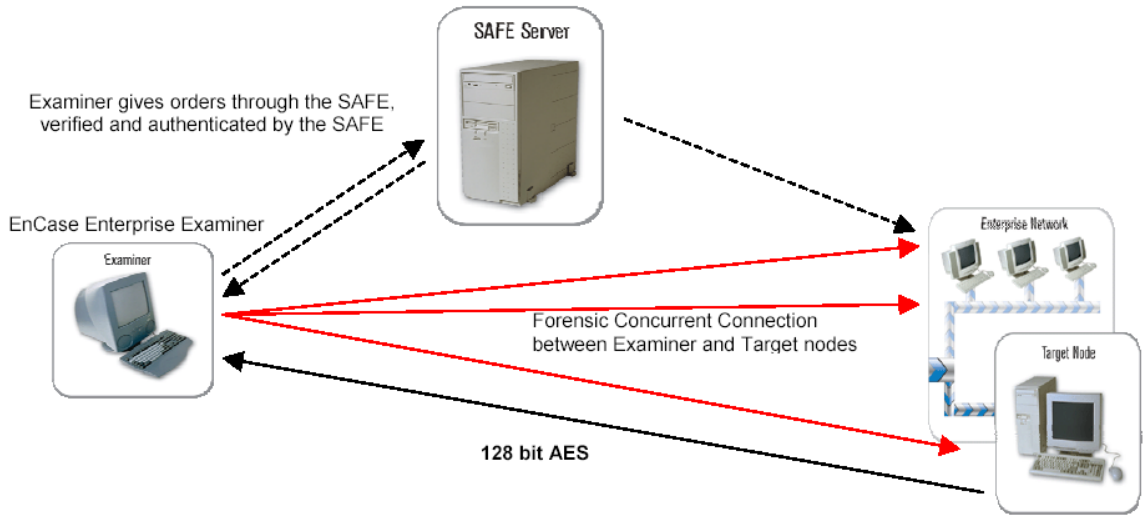

Figure 1 EnCase Enterprise components and Forensic Concurrent connection logical representation

Incident Response Concurrent Connections (Snapshot): A secure virtual connection that is spawned temporarily from the SAFE server to target machines then onto the Examiner. The number of Snapshot connections controls how quickly an organization can audit their environment for malicious or unauthorized activity. Snapshot captures volatile data, providing information on what was occurring on a system at a given point in time.

The ability to immediately capture volatile data assists investigators and Computer Incident Response Teams (CIRTs) in quickly identifying the scope, magnitude, and status of suspected incidents. This capability, along with the ability to quickly preview and validate static files on system media, gives administrators the ability to quickly isolate, identify, assess, and remediate internal and external security breaches. Volatile data harvested by Snapshot consists of: open ports; active processes; open files; Live Windows Registry; network users; and network interfaces.

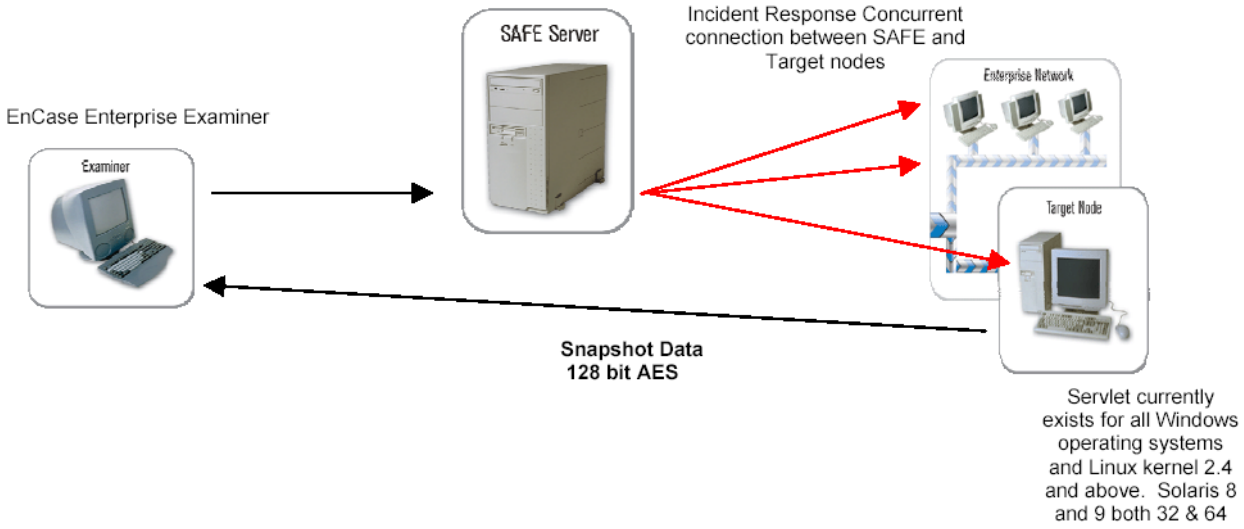

Figure 2 EnCase Enterprise components and Incident Response (Snapshot) Concurrent connection logical representation

2.2.1 Physical Boundaries

EnCase Enterprise is composed of three components: SAFE; Examiner; and Servlets. Each component is a separately installed software package. The SAFE server and the Examiner client require the presence of a physical hardware security key (or "dongle"). The dongle is a USB thumb drive that is supplied with the TOE for license enforcement. The dongle is not a security enforcing component.

- The SAFE component controls access to the Servlets.
- The Examiner component includes the network investigation tools.
- The Servlet component is the agent running on the targeted network workstations and servers.

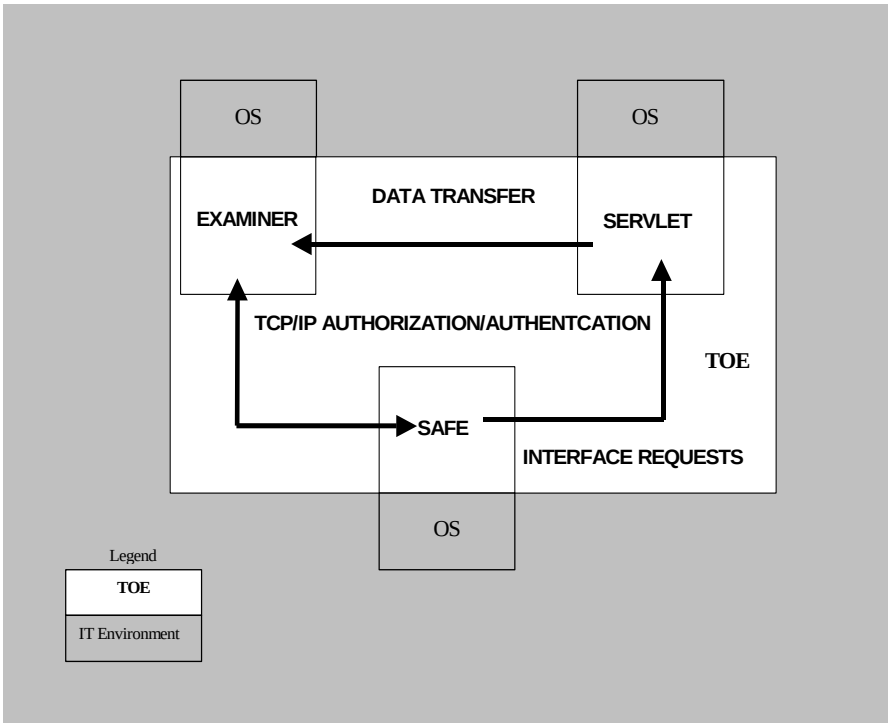

Figure 3 EnCase Enterprise High Level Overview Diagram

2.2.2 Logical Boundaries

The logical boundaries are the security functions provided by the TOE.

2.2.2.1 Security audit

The TOE generates log files of the transactions that occur at the SAFE. Audit logs include information for each audited event, including the identity of the responsible user. The TOE offers the ability for authorized administrators to perform an audit log review.

2.2.2.2 Cryptographic Support

The TOE cryptographic capabilities are provided by the EnCase Enterprise Cryptographic Module 1.0, which is a FIPS 140-2 validated cryptographic module (certificate #942).

Note, to support the key generation the cryptographic module relies on the RNG functionality of the FIPS 186-2 based Microsoft Enhanced Cryptographic Provider (Cryptographic Application Programming Interface CAPI), which earned certificate number 238 and is provided by the IT environment.

2.2.2.3 User data protection

EnCase Enterprise restricts access to the Servlets running on the network resources (target nodes). Access is based upon the role assigned to the user.

2.2.2.4 Identification and authentication

EnCase Enterprise ensures users are identified and authenticated prior to allowing them the ability to access the TOE's security functions. Users are identified with a user name and authenticated with a password. User's attributes include: user name; authentication data (password); role; permissions; and permitted node IP addresses.

2.2.2.5 Security management

The TOE provides two security-roles: Keymaster; and administrators[1]. The TOE provides the Keymaster and authorized administrator with a graphical user interface (GUI) that can be used to configure and modify the options of the TOE. There are several modules available to the authorized administrator, such as manage user accounts and modify the behavior of the Access Control Policy. EnCase Enterprise restricts the ability to modify the behavior of the TOE to authorized administrators.

2.2.2.6 Protection of the TSF

As a product that is inherently spread out across a network, information passed between separate parts of the TOE are encrypted to ensure that information is neither intercepted, nor modified between two parts of the system. In addition, the TOE ensures that the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed

2.3 TOE Documentation

The EnCase Enterprise Version 6.8 Admin Manual, EnCase Enterprise Version 6.8 User Manual, and EnCase Enterprise Version 6.8 User Documentation Errata Sheet describe how to install and administer the TOE. Refer to Section 6.2 for information about these and other documents associated with the TOE.

[1] *For clarification, the two" security-roles" refer to "roles" as defined in the CC security functional requirement FMT_SMR.1. In this case, the Keymaster is a superuser of the TOE, while the administrators are all other operators of the TOE. Further usage of the term "role(s)" will refer to the manner in which the TOE groups administrators based on the permissions they have been assigned and the types of duties they have been tasked to perform. Further instances of "user" will refer to administrators that do not fall under a more specific category*

3. Security Environment

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

The statement of the TOE security environment defines the following:

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

3.1 Threats

T.ACCESS	Users may gain access to the functions of the TOE to which they are not authorized.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.TRANSIT	An unauthorized user may eavesdrop on communications between separate parts of the TOE allowing them to intercept and modify transmitted information.

3.2 Assumptions

3.2.1 Physical Assumptions

A.PROTECT	The components of the TOE critical to security policy enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.
A.TIME	The TOE's IT environment will provide a reliable time source to enable the TOE to timestamp audit records.

3.2.2 Personnel Assumptions

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 authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

3.3 Organizational Security Policies

P.ACCACT	Users of the TOE shall be accountable for their actions within the network.
P.GEN_KEYS	Cryptographic keys will be generated in accordance with requirements defined by FIPS 140-2.
P.DES_KEYS	Cryptographic keys will be destroyed in accordance with requirements defined by FIPS 140-2.
P.MANAGE	The TOE must provide authorized administrators with utilities to effectively manage the security-related functions of the system.
P.PROTECT	The TOE shall be protected from unauthorized accesses and modification of TOE data and functions.

4. Security Objectives

This section defines the security objectives of the TOE and its supporting environment. Security objectives, categorized as either IT Security Objectives for the TOE, IT Security Objectives for the Environment, or Non-IT Security Objectives for the Environment, reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified, and address the identified assumptions. All of the identified threats, assumptions, and organizational policies are addressed under one of the categories below.

4.1 Security Objectives for the TOE

O.AUDITS	The TOE must record audit records for data accesses and use of the TOE functions.
O.AUTH	The TSF must ensure that only authorized users gain access to the TOE and its resources by uniquely identifying and authenticating all users before granting access to the TOE and its resources.
O.CONTROL	The TSF must control access to the TOE and its resources based on subject's identification. The TSF must provide the ability to limit each subject's access.
O.CRYPTO_DEST	The TSF must ensure that cryptographic keys are destroyed in accordance with requirements defined by FIPS 140-2.
O.CRYPTO_OPS	The TSF must ensure that all cryptographic operations used to protect information and encryption keys meet the standards defined by FIPS 140-2.
O.DATA_TRANSFER	The TSF must have the capability to protect TSF data in transmission between distributed parts of the TOE.
O.MANAGE	The TOE 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.PROTECT	The TOE shall be protected from unauthorized accesses and modification of TOE data and functions.

4.2 Security Objectives for the IT Environment

O.CRYPTO_GEN	The TOE's IT environment must ensure that cryptographic keys are generated in accordance with requirements defined by FIPS 140-2.
O.TIME	The TOE's IT environment must provide a reliable time source for the TOE to provide accurate timestamps for audit records.
O.TOE_PROTECTION	The IT Environment will protect the TOE and its assets from interference or tampering.

4.3 Security Objectives for the Non-IT Environment

OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.PERSON	Authorized administrators of the TOE shall be properly trained in the configuration and usage of the TOE and will follow the guidance provided. These users are not careless, negligent, or hostile.
OE.PHYCAL	Those responsible for the TOE must ensure that the parts of the TOE critical to security policy are protected from physical attack and modification that might compromise the TOE security objectives.

5. IT Security Requirements

This section defines the security functional requirements for the TOE as well as the security assurance requirements against which the TOE has been evaluated. The SFRs were drawn from Part 2 of the Common Criteria, version 2.3.

The overall strength of function claim for the TOE is SOF-basic. The only security functional requirements that are associated with permutational or probabilistic mechanisms are related to user authentication (FIA_UAU.2) and encryption (FPT_ITT.1).

5.1 TOE Security Functional Requirements

The following table describes the SFRs that are satisfied by EnCase Enterprise.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit data generation
	FAU_GEN.2: User identity association
	FAU_SAR.1: Audit review
FCS: Cryptographic support	FCS_CKM.4: Cryptographic key destruction
	FCS_COP.1a: Cryptographic operation
	FCS_COP.1b: Cryptographic operation
FDP: User data protection	FDP_ACC.2: Complete access control
	FDP_ACF.1: Security attribute based access control
FIA: Identification and authentication	FIA_ATD.1: User attribute definition
	FIA_UAU.2: User authentication before any action
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MSA.1: Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_MTD.1: Management of TSF data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_ITT.1: Basic internal TSF data transfer protection
	FPT_RVM.1: Non-bypassability of the TSP

Table 1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1)

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

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

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

c) **[login, logoff, connected to a Servlet, disconnected from a Servlet, start a snapshot, stop a snapshot, failed connection to a Servlet, user creation, user modification, user deletion, SAFE service stop, SAFE service start]**.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[no additional information]**.

5.1.1.2 User identity association (FAU_GEN.2)

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

5.1.1.3 Audit review (FAU_SAR.1)

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

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

1.1.1 Cryptographic support (FCS)

5.1.1.4 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[zeroization]** that meets the following: **[FIPS 140-2]**.

5.1.1.5 Cryptographic operation (FCS_COP.1a)

FCS_COP.1a.1 The TSF shall perform **[symmetric encryption and decryption]** in accordance with a specified cryptographic algorithm **[AES]** and cryptographic key sizes **[128-bit AES symmetric]** that meet the following: **[FIPS 197]**.

5.1.1.6 Cryptographic operation (FCS_COP.1b)

FCS_COP.1b.1 The TSF shall perform **[digital signature generation and verification]** in accordance with a specified cryptographic algorithm **[DSA]** and cryptographic key sizes **[1024]** that meet the following: **[FIPS 186-2]**.

5.1.2 User data protection (FDP)

5.1.2.1 Complete access control (FDP_ACC.2)

FDP_ACC.2.1 The TSF shall enforce the **[Access Control Policy]** on **[subject: users, objects: nodes in which Servlet has been installed]** 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 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the **[Access Control Policy]** to objects based on the following:
[subject: users
subject security attributes: role, permitted node IP addresses
objects: nodes in which Servlet has been installed
object security attribute: node IP address].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[access to the node is granted if the node IP address is contained in the subject's list of permitted node IP addresses, and if the subject's assigned role allows the requested action]**.

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

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

5.1.3 Identification and authentication (FIA)

5.1.3.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **[user name, authentication data, admin permission, role, permitted node IP addresses]**.

5.1.3.2 User authentication before any action (FIA_UAU.2)

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

5.1.3.3 User identification before any action (FIA_UID.2)

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

5.1.4 Security management (FMT)

5.1.4.1 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the **[Access Control Policy]** to restrict the ability to **[*query, modify, delete*]** the security attributes **[roles, permissions, permitted node IP addresses]** to **[Administrator]**.

5.1.4.2 Static attribute initialization (FMT_MSA.3)

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

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

5.1.4.3 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to **[*query, modify, delete*]** the **[role, permission and permitted node IP addresses security attributes belonging to individual users]** to **[Administrator]**.

5.1.4.4 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **[manage security attributes, manage the Access Control Polices]**.

5.1.4.5 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles **[Keymaster and Administrator]**.

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 Basic internal TSF data transfer protection (FPT_ITT.1)

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

5.1.5.2 Non-bypassability of the TSP (FPT_RVM.1)

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

This section specifies the security functional requirements (SFRs) for the IT Environment. This section organizes the SFRs, drawn from Part 2 of the Common Criteria, version 2.3, by CC class. Table 2 identifies all SFRs implemented by the IT Environment and indicates the ST operations performed on each requirement.

Requirement Class	Requirement Component
FCS: Cryptographic support	FCS_CKM.1: Cryptographic key generation
FPT: Protection of the TSF	FPT_SEP.1: TSF domain separation
	FPT_STM.1: Reliable time stamps

Table 2 Security Functional Components for the IT Environment

5.2.1 Cryptographic support (FCS)

5.2.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The ~~TSF~~ **IT Environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[DSA]** and specified cryptographic key sizes **[1024-bit]** that meet the following: **[FIPS 186-2]**.

5.2.2 Protection of the TSF (FPT)

5.2.2.1 TSF domain separation (FPT_SEP.1)

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

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

5.2.2.2 Reliable time stamps (FPT_STM.1)

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

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 components as specified in Part 3 of the Common Criteria, version 2.3. No operations are applied to the assurance components.

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

Table 3 EAL 2 Assurance Components

5.3.1 Configuration management (ACM)

5.3.1.1 Configuration items (ACM_CAP.2)

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

5.3.2 Delivery and operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2d The developer shall use the delivery procedures.
ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

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

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

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

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

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

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

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

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

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

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

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

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

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

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

5.3.3.2 Descriptive high-level design (ADV_HLD.1)

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

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

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

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

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

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

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

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

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

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

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

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

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

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

5.3.4.2 User guidance (AGD_USR.1)

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

5.3.5 Tests (ATE)

5.3.5.1 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1d The developer shall provide evidence of the test coverage.
ATE_COV.1.1c The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.

ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.
ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.3 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.
ATE_IND.2.1c The TOE shall be suitable for testing.
ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.6 Vulnerability assessment (AVA)

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

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.
AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.
AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.6.2 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.
AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.
AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.
AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.
AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
AVA_VLA.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Security audit

The TOE generates log files of the transactions that occur at the SAFE, which are security-related events. These events are tied to the administrator that performed the action, as well as the action performed, and the time it was performed. These audit records are stored in the SAFE server where the authorized administrator can view the logs. The audit records include SAFE Server-related events such as user creation, user modification, user deletion, SAFE service stop/start. Audit records also include Examiner-related events such as login, logoff, connected to a Servlet, disconnected from a Servlet, start a snapshot, stop a snapshot, and failed connection to a node. All audit records include the following information: date and time of the event, the type of event, the subject identity, and the outcome of the event (failure or success). The time stamp included in the audit record is taken from the operating system it is running on. This audit data is presented in such a manner that the authorized administrator can read and interpret the content of the information; hence the information is presented in a manner suitable for human interpretation.

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

- FAU_GEN.1: Audit data generation
- FAU_GEN.2: User identity association
- FAU_SAR.1: Audit review.

6.1.2 Cryptographic Support

The TOE uses the EnCase Enterprise Cryptographic Module 1.0 to provide the cryptographic capabilities. The cryptography module is FIPS 140-2 validated, certificate #942.

The keys are used solely to protect the communication between the TOE components. To support the key generation, the cryptographic module relies on the RNG functionality of the FIPS 186-2 based Microsoft Enhanced Cryptographic Provider (Cryptographic Application Programming Interface CAPI), which is provided by the IT environment. The Examiner component exports the keys to the SAFE component. For the target nodes, Servlets are deployed as services that run with administrative privileges on each target node (machine). The Servlet accepts commands from the Examiner client; these requests are signed by the SAFE server and verified by the network device. The Servlet contains the SAFE server's public key.

When the user account is removed from the system, the associated keys are zeroized in accordance with FIPS 140-2.

The Cryptographic support security function is designed to satisfy the following security functional requirements:

- FCS_CKM.4: Cryptographic key destruction
- FCS_COP.1a,b: Cryptographic operation.

6.1.3 User data protection

The User data protection function covers the Access Control Policy. The policy restricts access to Servlets based upon the role and the permitted node IP addresses assigned to the user. The TOE also restricts actions that can be performed on the Servlets. A user can be assigned to multiple roles and all permissions are administrative type permissions. The permissions are role-based permissions, giving granular access control for ensuring proper enforcement of policies.

For example, a user assigned Investigator1 role can only access Servlets 1, 3, and 5 while another user that is assigned Investigator2 role can only access Servlets 2, 4, and 6. In addition to the role, permissions are also assigned that restrict the actions a particular role can perform. Using the same roles (two separate users), Investigator1 has been granted browse file structures on the Servlets while Investigator2 can browse file structures, view file content, and perform keyword search on the Servlets to which access has been granted. Therefore, using the example, the only permissions Investigator1 role has are to browse the file structures on Servlets 1, 3, and 5. The TOE identifies Servlets by their IP addresses.

As seen in the above example, the actions that can be performed on a particular Servlet also depend on the permissions granted to the role. The permissions that can be granted to each role are: Acquire Image; Browse File Structure; View File Contents; View Pictures; Copy Files; Keyword Search; Allow Script File Access; Allow Registry Value Access; Allow Registry List Access; and Snapshot Information. Snapshot information includes open ports, active processes, open files, Live Windows Registry, network users, and network interfaces.

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

- FDP_ACC.2: Complete access control
- FDP_ACF.1: Security attribute based access control.

6.1.4 Identification and authentication

The TOE maintains user accounts for the authorized users of the system. The user accounts maintain the following attributes; user name, authentication data (passwords), role, permitted node IP addresses, and permissions. The role attribute does not indicate a security role as defined in FMT_SMR.1. Role is synonymous with groups. Roles can be utilized to distinguish different user groups, such as investigators, reviewers, etc.

The TOE does not allow any action to be performed on behalf of the user before the user is successfully identified and authenticated. Each user's identity must be verified via successful authentication; by providing the correct password associated with the user identity before any TSF-mediated action is allowed. This security function has a SOF-basic strength of function claim.

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

- FIA_ATD.1: User attribute definition
- FIA_UAU.2: User authentication before any action
- FIA_UID.2: User identification before any action.

6.1.5 Security management

The TOE supports two security management roles: Keymaster; and Administrator.

The Keymaster is the super administrator for the SAFE Server. During installation of the SAFE, a Keymaster account is created. After installation, the Keymaster is the only person with the ability to log on to the SAFE until other user accounts are created. Due to the authority the Keymaster has on the system, it is recommended that the Keymaster not be a regular user of the SAFE. Instead, the Keymaster is intended to delegate the day-to-day administration of the TOE to users that the Keymaster creates. The Keymaster can grant any and all permission and authority that the Keymaster has to any administrator, except for the ability to delete the Keymaster. This ensures that the TOE can be properly administered in the absence of the Keymaster.

All other users are considered administrators. The user permissions are all administrative type permissions. If a user is not given any user permissions, they can log on to the SAFE, but they cannot perform any functions using the interface. User accounts are given permissions using roles. A user account can be given multiple roles, so when the user starts a new case they choose which role they want to use from the pool of roles assigned to them. Access can be further defined by timeframe controls: role start; role expires; and hours.

The TSF provides the ability to manage the security functions of the TOE. Only administrators authorized by the Keymaster are permitted to perform management functions. The management functions include the ability to query, modify, and/or delete the security attributes: roles, permissions and target nodes associated with the Access Control Policy. Administrators can dictate what nodes a particular user has access to, based on the target node's IP address, and what functions they are allowed to perform on those specific nodes on a case-by-case basis.

By default, users do not have permissions to perform any actions until the administrator assigns roles and permissions to the user's account. The permissions can be categorized as follows:

- admin permissions—they grant users the ability to perform administrative functions on the TOE (create users, create roles, edit network layout, view logs, remote logon, allow remote logon). These permissions are granted directly to a user, the user does not have to be allocated a role.
- role permissions—they define the capabilities of roles that are created by the administrator and assumed by users performing investigations. These permissions can only be granted by granting a user a role that contains "role permissions", they are not granted directly to the user.

The "admin permissions" define administrator capabilities and are part of security management, while the "role permissions" define user authorizations and are part of User Data Protection.

The TOE does not provide the ability to change this default to a more permissive value during creation, therefore no user role can specify alternative initial values to override the default values when a user's account is created.

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

- 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.

6.1.6 Protection of the TSF

The TOE ensures that the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. The TSF requires that all users be successfully identified and authenticated before they are allowed to view or modify the TSP. Once these steps are completed successfully, the authorized user only has access to functions as specified by his or her assigned role and permissions.

To protect data from disclosure and modification that is transferred between the TOE components, all data transferred between the Examiner component and the SAFE component, between the SAFE and the target node, and between the target node and the Examiner component is encrypted. Using encrypted data streams for communications ensures that the transferred data is protected from disclosure and modification. This is sufficient to maintain the integrity of the data that is being transferred.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_ITT.1: Basic internal TSF data transfer protection
- FPT_RVM.1: Non-bypassability of the TSP.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by Guidance Software ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Guidance Software ensures changes to the implementation representation are controlled. Guidance Software

performs configuration management on the TOE implementation representation, design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, vulnerability analysis documentation, and configuration management documentation.

These activities are described in the following documentation:

- Guidance Software Product Development Lifecycle (ACM), Version 2, 20 June 2008.

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

- ACM_CAP.2.

6.2.2 Delivery and operation

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

These activities are documented in:

- Guidance Software Production Manual, 18 September 2005
- Guidance Software Customer Service Manual, 25 August 2004
- EnCase Enterprise Version 6.8 Admin Manual, 2007
- EnCase Enterprise Version 6.8 User Manual, 2007.

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

- ADO_DEL.1
- ADO_IGS.1.

6.2.3 Development

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

These activities are documented in:

- Target of Evaluation (TOE) Security Functions (ADV), Version 3, 20 June 2008
- EnCase® Enterprise Subsystems, Version 2, 20 June 2008
- EnCase Enterprise Edition Security Protocols, 2005.

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

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

6.2.4 Guidance documents

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

These activities are documented in:

- EnCase Enterprise Version 6.8 Admin Manual, 2007
- EnCase Enterprise Version 6.8 User Manual, 2007
- EnCase Enterprise Version 6.8 User Documentation Errata Sheet, 2008.

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

- AGD_ADM.1
- AGD_USR.1.

6.2.5 Tests

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

These activities are documented in:

- EnCase 6.8 Quality Assurance Test Plan, Version 1.0, 11 June 2008
- TOE Security Function Test Suite, 4 June 2008
- TOE Security Function Test Suite – Revision 2, 26 August 2008.

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

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

6.2.6 Vulnerability assessment

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

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

These activities are documented in:

- EnCase® Enterprise Vulnerability Assessment, Version 1, 20 June 2008
- EnCase® Enterprise Strength of Function Analysis, Version 1, 20 June 2008.

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

- AVA_SOF.1
- AVA_VLA.1.

7. Protection Profile Claims

There is no Protection Profile claim in this Security Target.

8. Rationale

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

- Security Objectives
- Security Functional Requirements
- Internal Consistency
- Security Assurance Requirements
- Strength of Functions
- Requirement Dependencies
- Explicitly Stated Requirements
- TOE Summary Specification
- PP Claims.

8.1 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and policy statement. The following table demonstrates that the mapping between the assumptions, threats, and polices to the security objectives is complete. The discussion following provides the rationale of coverage for each assumption, threat, and policy.

8.1.1 Security Objectives Rationale for the TOE and Environment

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

	O.AUDITS	O.AUTH	O.CONTROL	O.CRYPTO_DEST	O.CRYPTO_OPS	O.DATA_TRANSFER	O.MANAGE	O.PROTECT	O.CRYPTO_GEN	O.TIME	O.TOE_PROTECTION	OE.INSTAL	OE.PERSON	OE.PHYCAL
T.ACCESS		X	X					X						
T.PRIVIL		X	X					X			X			
T.TRANSIT					X	X								
A.PROTCT											X			X
A.TIME										X				
A.MANAGE													X	X
A.NOEVIL												X	X	
P.ACCACT	X	X						X						
P.GEN_KEYS									X					
P.DES_KEYS				X										
P.MANAGE		X					X						X	
P.PROTECT		X					X	X				X		X

Table 4 Security Environment vs. Objectives

8.1.1.1 T.ACCESS

Users may gain access to the functions of the TOE to which they are not authorized.

This Threat is satisfied by ensuring that:

- O.CONTROL – This objective counters the threat T.ACCESS by limiting each subject's access to the TOE and its resources.
- O.AUTH – The TSF must ensure that only authorized users gain access to the TOE and its resources by uniquely identifying and authenticating all users before granting access to the TOE and its resources.
- O.PROTECT – TOE must protect its functions by ensuring its security functions cannot be bypassed.

8.1.1.2 T.PRIVIL

An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

This Threat is satisfied by ensuring that:

- O.AUTH – This objective ensures that only authorized users have access to the TOE and its resources by uniquely identifying and authenticating all users before granting access.
- O.CONTROL – This objective counters the threat T.PRIVIL by requiring each user (subject) be identified before any access to the TOE and its protected resources is granted.
- O.PROTECT – This objective ensures security functions cannot be bypassed.
- O.TOE_PROTECTION – This security objective further protects the TOE from inappropriate access as well as protecting application components from interference or tampering.

8.1.1.3 T.TRANSIT

An unauthorized user may eavesdrop on communications between separate parts of the TOE allowing them to intercept and modify transmitted information.

This Threat is satisfied by ensuring that:

- O.CRYPTO_OPS – This objective ensures that all data transmitted is encrypted.
- O.DATA_TRANSFER – This objective ensure that communications between TOE components are protected.

8.1.1.4 A.PROTCT

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

This Assumption is satisfied by:

- OE.PHYCAL – This objective provides for the physical protection of the TOE.
- O.TOE_PROTECTION – This security objective further protects the TOE from inappropriate access as well as protecting application components from interference or tampering.

8.1.1.5 A.TIME

The TOE's IT environment will provide a reliable time source to enable the TOE to timestamp audit records.

This Assumption is satisfied by:

- O.TIME – This objective ensures the IT environment provides a reliable time source for the TOE to provide an accurate timestamp for all audit records.

8.1.1.6 A.MANAGE

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

This Assumption is satisfied by:

- OE.PERSON – This objective ensures all authorized administrators are qualified and trained to manage the TOE.
- OE.PHYCAL – Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

8.1.1.7 A.NOEVIL

The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

This Assumption is satisfied by:

- OE.INSTAL – Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
- OE.PERSON – Authorized administrators of the TOE shall be properly trained in the configuration and usage of the TOE and will follow the guidance provided. These users are not careless, negligent, or hostile.

8.1.1.8 P.ACCACT

Users of the TOE shall be accountable for their actions within the network.

This Organizational Security Policy is satisfied by:

- O.AUDITS – This objective implements this policy by requiring auditing of all data accesses and use of TOE functions.
- O.AUTH – This objective supports this policy by ensuring each user is uniquely identified and authenticated.
- O.PROTECT – This objective ensures the TOE and its data are protected from unauthorized accesses and modification.

8.1.1.9 P.GEN_KEYS

Cryptographic keys will be generated in accordance with requirements defined by FIPS 140-2.

This Organizational Security Policy is satisfied by:

- O.CRYPTO_GEN – This objective ensures that keys are generated in accordance FIPS 140-2.

8.1.1.10 P.DES_KEYS

Cryptographic keys will be destroyed in accordance with requirements defined by FIPS 140-2.

This Organizational Security Policy is satisfied by:

- O.CRYPTO_DEST – This objective ensures that keys are zeroized in accordance with FIPS 140-2.

8.1.1.11 P.MANAGE

The TOE must provide authorized administrators with utilities to effectively manage the security-related functions of the system.

This Organizational Security Policy is satisfied by:

- O. AUTH – This objective ensures each user is uniquely identified and authenticated prior to any TOE function accesses.
- O.MANAGE – This objective ensures there is a set of functions for administrators to use and that only authorized administrators have access to such functionality.
- OE.PERSON – This objective ensures competent administrators will manage the TOE.

8.1.1.12 P.PROTECT

The TOE shall be protected from unauthorized accesses and modification of TOE data and functions.

This Organizational Security Policy is satisfied by:

- O. AUTH – This objective ensures each user is uniquely identified and authenticated prior to any TOE function accesses.
- O.MANAGE – This objective ensures there is a set of functions for administrators to use and that only authorized administrators have access to such functionality.
- O.PROTECT – This objective ensures the TOE and its data are protected from unauthorized accesses and modification.
- OE.INSTAL – This objective ensures that the TOE is properly installed and operated.
- OE.PHYCAL – Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

8.2 Security Requirements Rationale

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

8.2.1 Security Functional Requirements Rationale

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

	O.AUDITS	O.AUTH	O.CONTROL	O.CRYPTO_DEST	O.CRYPTO_OPS	O.DATA_TRANSFER	O.MANAGE	O.PROTECT	O.CRYPTO_GEN	O.TIME	O.TOE_PRTOECTION
FAU_GEN.1	X										
FAU_GEN.2	X										
FAU_SAR.1	X										
FCS_CKM.1									X		
FCS_CKM.4				X							
FCS_COP.1a,b					X						
FDP_ACC.2			X								
FDP_ACF.1			X								
FIA_ATD.1			X								
FIA_UAU.2		X									
FIA_UID.2		X									
FMT_MSA.1							X				
FMT_MSA.3							X				
FMT_MTD.1							X				
FMT_SMF.1							X				
FMT_SMR.1							X				
FPT_ITT.1						X					
FPT_RVM.1			X					X			
FPT_SEP.1											X
FPT_STM.1										X	

Table 5 Objective to Requirement Correspondence

8.2.1.1 O.AUDITS

The TOE must record audit records for data accesses and use of the TOE functions.

This TOE Security Objective is satisfied by:

- FAU_GEN.1 and FAU_GEN.2 requirements define the TOE events that will be audited, along with the details that will be recorded for each event.
- FAU_SAR.1 provides administrators with access to view the audit trail.

8.2.1.2 O.AUTH

The TSF must ensure that only authorized users gain access to the TOE and its resources by uniquely identifying and authenticating all users before granting access to the TOE and its resources.

This TOE Security Objective is satisfied by:

- FIA_UID.2 requirement requires a user be identified before any access to the TOE and TOE-protected resources is allowed
- FIA_UAU.2 requirement requires a user be authenticated before any access to the TOE and TOE-protected resources is allowed

8.2.1.3 O.CONTROL

The TSF must control access to the TOE and its resources based on subject's identification. The TSF must provide the ability to limit each subject's access.

This TOE Security Objective is satisfied by:

- FIA_ATD.1 requirement defines the unique attributes that are associated with individual users.
- FDP_ACC.2 and FDP_ACF.1 requirements require the TOE to prevent unauthorized access to target nodes.
- FPT_RVM.1 ensures that the TOE security policies cannot be bypassed since the TOE restricts all access to the target nodes to which the user has not been granted access.

8.2.1.4 O.CRYPTO_DEST

The TSF must ensure that cryptographic keys are destroyed in accordance with requirements defined by FIPS 140-2.

This TOE Security Objective is satisfied by:

- FCS_CKM.4: This requirement ensures that keys are destroyed in accordance with FIPS 140-2.

8.2.1.5 O.CRYPTO_OPS

The TSF must ensure that all cryptographic operations used to protect information and encryption keys meet the standards defined by FIPS 140-2.

This TOE Security Objective is satisfied by:

- FCS_COP.1: This requirement ensures the operation of data encryption and decryption is performed in accordance with FIPS 140-2.

8.2.1.6 O.DATA_TRANSFER

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

This TOE Security Objective is satisfied by:

- FPT_ITT.1: The TOE ensures that data transmission between TOE components is protected from disclosure and modification.

8.2.1.7 O.MANAGE

The TOE 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.

This TOE Security Objective is satisfied by:

- FMT_MSA.1: This requirement restricts the ability to manage the associated security attributes.
- FMT_MSA.3: The TOE ensures restrictive default settings for new users.
- FMT_SMR.1: Requires that the TOE provide the ability to maintain roles for security relevant authority: Keymaster and administrator.
- FMT_MTD.1: Ensures that only the authorized administrator can change the permissions of other administrators.
- FMT_SMF.1: Requires that the TOE provide the ability to manage its security functions including the management of security attributes and management of the access control policy.

8.2.1.8 O.PROTECT

The TOE shall be protected from unauthorized accesses and modification of TOE data and functions.

This TOE Security Objective is satisfied by:

- FPT_RVM.1: Ensures that all operations of the TOE are subject to TSP enforcement.

8.2.1.9 O.CRYPTO_GEN

The TOE's IT environment must ensure that cryptographic keys are generated in accordance with requirements defined by FIPS 140-2.

This IT Environment Security Objective is satisfied by:

- FCS_CKM.1: This requirement ensures that the IT environment generates keys in accordance with FIPS 140-2 using a pseudo random number generator.

8.2.1.10 O.TIME

The TOE's IT environment must provide a reliable time source for the TOE to provide accurate timestamps for audit records.

This IT Environment Security Objective is satisfied by:

- FPT_STM.1 ensures that an accurate time source will be available to the TOE

8.2.1.11 O.TOE_PROTECTION

The IT Environment will protect the TOE and its assets from interference or tampering.

This IT Environment Security Objective is satisfied by:

- FPT_SEP.1 ensures the IT environment provides a secure runtime environment for the TOE.

8.3 Internal Consistency Rationale

The ST includes no instance of a requirement that contradicts another requirement in the ST. In instances where different requirements apply to the same events or types of data, the requirements and the operations performed within the requirements do not contradict each other, but provide supporting functionality ensuring that the TOE is internally consistent.

The combination of several different supporting security functions, and the inclusion of all dependencies as illustrated in Table 6 Requirement Dependency Rationale ensures that together the selected requirements form a mutually supportive whole. The following items also support this claim:

- Mapping and suitability of the requirements to security objectives (as justified in Table 5 Objective to Requirement Correspondence);
- Inclusion of identification and authentication to ensure only authorized users access the TOE functions and its data; and
- Inclusion of security management requirements to ensure proper configuration and control of other security functional requirements.

8.4 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL2 assurance package. The EAL chosen is based on the statement of the security environment (assumptions, organizational security policies, and threats) and the security objectives defined in this ST. The sufficiency of the EAL chosen (EAL2) 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.MANAGE and A.NOEVIL). The TOE is physically protected (OE.PHYCAL) and is properly and securely configured (OE.INSTAL). Given these aspects, a TOE based on good commercial development practices is sufficient. EAL 2 is an appropriate level of assurance for the TOE described in this ST. As such, it is believed that EAL2 provides an appropriate level of assurance in the security functions offered by the TOE.

8.5 Strength of Functions Rationale

The claimed TOE minimum strength of function is SOF-basic. This strength of function level was selected because it generally corresponds with the claimed assurance level of EAL 2 assurance package.

The TOE includes security functional requirements that have a specific strength of function metrics or a mechanism of a probabilistic or permutational nature. Of those requirements; FCS_CKM.1 and FCS_COP.1 are cryptographic mechanisms, which is outside the scope of the evaluation.

The password mechanism is of a probabilistic or permutational nature. The password mechanism is used in the Identification and Authentication security function to authenticate user identity. The relevant security functional requirement is FIA_UAU.2. The intent is that the password mechanism meets or exceeds SOF-basic and the evidence can be found in the strength of function analysis included in the EnCase® Enterprise Strength of Function Analysis document.

8.6 Requirement Dependency Rationale

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

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1 (IT Environment)
FAU_GEN.2	FAU_GEN.1 and FIA_UID.1	FAU_GEN.1 and FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1) and FCS_CKM.4 and FMT_MSA.2	FCS_COP.1a,b and FCS_CKM.4 (absence of FMT_MSA.2 is rationalized at the end of this section)
FCS_CKM.4	(FDP_ITC.1 or FCS_CKM.1) and FMT_MSA.2	FCS_CKM.1 (IT Environment) (absence of FMT_MSA.2 is rationalized at the end of this section)

ST Requirement	CC Dependencies	ST Dependencies
FCS_COP.1a,b	(FDP_ITC.1 or FCS_CKM.1) and FCS_CKM.4 and FMT_MSA.2	FCS_CKM.1 (IT Environment) and FCS_CKM.4 (absence of FMT_MSA.2 is rationalized at the end of this section)
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.2 and FMT_MSA.3
FIA_ATD.1	None	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	None	None
FMT_MSA.1	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_ACC.2
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1 and FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_ITT.1	None	None
FPT_RVM.1	None	None
FPT_SEP.1	None	None
FPT_STM.1	None	None

Table 6 Requirement Dependency Rationale

For FCS_COP.1 requirement, the CC identifies the following dependency: FMT_MSA.2. The dependency for this requirement is not applicable. Following is the justification for not including this requirement:

- FMT_MSA.2: this requirement is concerned with ensuring that only secure values are accepted for security attributes. This only applies to the generation of the key pair. The administrator does not enter any values related to the cryptographic security function specified by FCS_COP.1. Therefore, this requirement is not applicable. Furthermore, the cryptographic module is FIPS 140-2 validated. The TOE uses this module exactly as specified by the FIPS 140-2 validation testing. Therefore, the dependencies of secure key values are satisfied by this module's validation as FIPS 140-2 compliant. Refer to certificate #942.

8.7 Explicitly Stated Requirements Rationale

There are no explicitly stated requirements in this Security Target.

8.8 TOE Summary Specification Rationale

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

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

	Security audit	Cryptographic support	User data protection	Identification and authentication	Security management	Protection of the TSF
FAU_GEN.1	X					
FAU_GEN.2	X					
FAU_SAR.1	X					
FCS_CKM.4		X				
FCS_COP.1a,b		X				
FDP_ACC.2			X			
FDP_ACF.1			X			
FIA_ATD.1				X		
FIA_UAU.2				X		
FIA_UID.2				X		
FMT_MSA.1					X	
FMT_MSA.3					X	
FMT_MTD.1					X	
FMT_SMF.1					X	
FMT_SMR.1					X	
FPT_ITT.1						X
FPT_RVM.1						X

Table 7 Security Functions vs. Requirements Mapping

8.9 PP Claims Rationale

See Section 7, Protection Profile Claims.