Secure Systems Limited Silicon Data Vault ® Security Target
September 7, 2005
Document No. F2-0805-004(1)

COACT, Inc.
Rivers Ninety Five
9140 Guilford Road, Suite N
Columbia, MD 21046-2587

Phone: 301-498-0150

Fax: 301-498-0855

DOCUMENT INTRODUCTION

Prepared By:

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

Prepared For:

Secure Systems Limited
Level 1, 80 Hasler Road,
Osborne Park
6017
Western Australia, Australia

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Secure Systems Limited Silicon Data Vault ® Laptop Version SDV18A03-A2-0003 and Secure Systems Limited Silicon Data Vault ® Desktop Version SDV201B03-0003. 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.

REVISION HISTORY

Rev	Description
	August 17, Initial Release
1	September 7, updates made to sections: 2.2, to address network connectivity in the IT environment 3.2.1, to address assumptions regarding network connectivity 4.2, to address objectives of the environment related to network connectivity 5.1.3.3, to add an application note to address remote authentication 5.1.3.5, to add an application note to address remote identification 8.1, to address new assumption/objective mappings and rationale

TABLE OF CONTENTS

1. SECURITY TARGET INTRODUCTION 1
1.1 Security Target Reference 1
1.1.1 Security Target Name 1
1.1.2 Security Target Author 1
1.1.3 Security Target Publication Date 1
1.1.4 TOE Reference 1
1.1.5 Evaluation Assurance Level 1
1.1.6 Keywords 1
1.2 ST Overview 1
1.2.1 Security Target Organisation 1
1.3 Common Criteria Conformance 2
1.4 Protection Profile Conformance 2
1.5 Security Target Conventions 2

2. TOE DESCRIPTION 3
2.1 Silicon Data Vault ® TOE Description 3
2.1.1 Physical Boundary 4
2.1.2 Logical Boundary 5
2.2 Silicon Data Vault ® IT-Environment 7

3. SECURITY ENVIRONMENT 9
3.1 Introduction 9
3.2 Assumptions 9
3.2.1 Personnel Assumptions 9
3.3 Threats 9
3.3.1 Threats Countered by the TOE 10
3.4 Organisational Security Policies 10

4. SECURITY OBJECTIVES 11
4.1 Security Objectives for the TOE 11
4.2 Security Objectives for the non-IT Environment 11
CHAPTER 5 13

5. IT SECURITY REQUIREMENTS 13
5.1 TOE Security Functional Requirements 13
5.1.1 Cryptographic Support (FCS) 14
5.1.1.1 FCS_CKM.1 Cryptographic Key Generation 14
5.1.1.2 FCS_CKM.4 Cryptographic Key Destruction 14
5.1.1.3 FCS_COP.1(a) Cryptographic Operation 14
5.1.1.4 FCS_COP.1(b) Cryptographic Operation 15
5.1.2 User Data Protection (FDP) 15
5.1.2.1 FDP_ACC.2 Complete Access Control 15
5.1.2.2 FDP_ACF.1-NIAP-0407 Security Attribute Based Access Control 15
5.1.3 Identification and Authentication (FIA) 16
5.1.3.1 FIA_AFL.1 Authentication Failure Handling 16
5.1.3.2 FIA_SOS.1 Verification of Secrets 16
5.1.3.3 FIA_UAU.2 User Authentication Before any Action 16

5.1.3.4 FIA_UAU.7 Protected Authentication Feedback 16
5.1.3.5 FIA_UID.2 User Identification Before any Action 17
5.1.4 Security Management (FMT) 17
5.1.4.1 FMT_MSA.1 Management of Security Attributes 17
5.1.4.2 FMT_MSA.3 Static Attribute Initialisation 17
5.1.4.3 FMT_SMF.1 Specification of Management Functions 17
5.1.4.4 FMT_SMR.1 Security Roles 17
5.1.5 Protection of the TSF (FPT) 18
5.1.5.1 FPT_RVM.1 Non-Bypassability of the TSP 18
5.1.5.2 FPT_SEP.1 TSF Domain Separation 18
5.2 TOE Security Assurance Requirements 18
5.3 Security Requirements for the IT Environment 19
5.4 Strength of Function Claims 19
5.5 Strength of Function Rationale 19

6. TOE SUMMARY SPECIFICATION 21
6.1 TOE Security Functions 21
6.2 TOE Security Function Rationale 23
6.3 Assurance Measures 24
6.4 Appropriate Strength of Function Claim 26

7. PROTECTION PROFILE CLAIMS 27
7.1 Protection Profile Reference 27
7.2 Protection Profile Refinements 27
7.3 Protection Profile Additions 27
7.4 Protection Profile Rationale 27

8. RATIONALE 29
8.1 Security Objectives Rationale 29
8.1.1 Rationale for TOE Security Objectives 29
8.1.2 Rationale for non-IT Environment Security Objectives 30
8.2 Security Requirements Rationale 30
8.2.1 Security Functional Requirements Mutually Supportive Whole Rationale 30
8.2.2 Security Functional Requirements Rationale for the TOE 30
8.2.3 Security Functional Requirements Rationale for the IT Environment 32
8.2.4 Security Assurance Requirements Rationale 32
8.2.5 Security Functional Requirements Dependencies Not Met Rationale 32
8.2.6 Explicit Security Functional Requirements Rationale 33
8.3 TOE Summary Specification Rationale 33
8.4 PP Claims Rationale 33

9. GLOSSARY OF TERMS 35

10. REFERENCES 37

LIST OF FIGURES

Figure 1 - Physical Boundary 5

LIST OF TABLES

Table 1 - Individual TOE Components 3

Table 2 - TOE SFRs 13

Table 3 - Assurance Requirements 18

Table 4 - Mappings Between TOE Security Functional Requirements and TOE Security Functions 23

Table 5 - Assurance Measures and Rationale 24

Table 6 - Mappings Between Assumptions, Threats, and Policies and Security Objectives 29

Table 7 - Mappings Between TOE Security Objectives and TOE Security Functional Requirements 31

ACRONYMS LIST

AES ..... Advanced Encryption Standard
CC ..... Common Criteria
CMVP ..... Cryptographic Module Validation Program
EAL2 ..... Evaluation Assurance Level 2
EMI/EMC ..... Electromagnetic Interference/Electromagnetic Compatibility
FIPS PUB ..... Federal Information Processing Standards Publication
FLASH ..... FLASH memory
HDD ..... Hard Disk Drive
IT ..... Information Technology
MBR ..... Master Boot Record
NIAP ..... National Information Assurance Partnership
OS ..... Operating System
PP ..... Protection Profile
PRNG ..... Psuedo Random Number Generator
RNG ..... Random Number Generator
SAU ..... System Administrator Utility
SDV ..... Silicon Data Vault ®
SF ..... Security Function
SFP ..... Security Function Policy
SHA-1 ..... Secure Hash Algorithm
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 Secure Systems Limited Silicon Data Vault ® Laptop Version SDV18A03-A2-0003 and Secure Systems Limited Silicon Data Vault ® Desktop Version SDV201B03-0003. 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 August 5, 2004 (tentative). As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

This section provides identifying information for the Secure Systems Limited Silicon Data Vault ® Security Target by defining the Target of Evaluation (TOE).

1.1.1 Security Target Name

Secure Systems Limited Silicon Data Vault ® Security Target, dated September 7, 2005.

1.1.2 Security Target Author

COACT, Inc.

1.1.3 Security Target Publication Date

September 7, 2005

1.1.4 TOE Reference

Secure Systems Limited Silicon Data Vault ® Laptop Version SDV18A03-A2-0003 and Secure Systems Limited Silicon Data Vault ® Desktop Version SDV201B03-0003. These version numbers uniquely identify the specific version of the TOE being evaluated.

1.1.5 Evaluation Assurance Level

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

1.1.6 Keywords

Encryption, Data Protection, Access Control, EAL 2

1.2 ST Overview

This Security Target defines the requirements for the Secure Systems Limited Silicon Data Vault ® Laptop Version SDV18A03-A2-0003 and Secure Systems Limited Silicon Data Vault ® Desktop Version SDV201B03-0003. The TOE is comprised of a suite of hardware, firmware and software that supports data encryption and hard disk partition access control. The TOE allows a System Administrator to dictate read/write access rights for authorised users of the TOE protected encrypted hard disk partitions.

1.2.1 Security Target Organisation

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 organisational 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 Secure Systems Limited Silicon Data Vault ® 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.

1.3 Common Criteria Conformance

The Secure Systems Limited Silicon Data Vault ® Laptop Version SDV18A03-A2-0003 and Secure Systems Limited Silicon Data Vault ® Desktop Version SDV201B03-0003, is compliant with the Common Criteria (CC) Version 2.2, functional requirements (Part 2) extended and assurance requirements (Part 3) conformant for EAL2.

1.4 Protection Profile Conformance

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

1.5 Security Target Conventions

Assignment: <u>Underlined</u>

Selection: *Italicised*

Refinement: **Bolded**

Assignment embedded within a selection: <u>*Underlined & Italicised*</u>

Iteration of a Security Requirement: Append with (x)

Explicitly Stated Requirements: Appended with _EXP.X

NIAP Explicitly Stated Requirements: Appended with -NIAP-####

CHAPTER 2

2. TOE Description

This section provides the context for the TOE evaluation by providing a description of the TOE including a description of the physical boundary of the TOE and logical boundary of the TOE.

2.1 Silicon Data Vault ® TOE Description

The TOE is a cryptographic and access control data protection device for desktop and laptop workstations that asserts absolute control over the host computer's hard disk drive (HDD) at the earliest stage of boot up, ensuring the user is authenticated before any data can be accessed.

The TOE is manufactured in two models, identified as the Secure Systems Limited Silicon Data Vault ® Laptop Version SDV18A03-A2-0003 and Secure Systems Limited Silicon Data Vault ® Desktop Version SDV201B03-0003. The functionality of the two models is identical with the only difference being the physical layout of the underlying hardware. This distinction allows the Secure Systems Limited Silicon Data Vault ® (SDV) to work on standard Desktop and Notebook (Laptop) computers. Both models execute the same underlying firmware and individual hardware components and are administered by the same management software. From this point the TOE will be referred to as the SDV Laptop or SDV Desktop for the laptop and desktop models of the TOE, respectively. In cases where information is relevant to both models, the TOE will simply be referred to as the SDV or the TOE.

As previously mentioned, both models of the TOE execute the same firmware and software components. The TOE part numbers identified in the previous paragraph correspond to the exact components listed in the table below. If one of these individual components were to change, the respective identified part number would change.

Table 1 - Individual TOE Components

Component Name	Component Version
TOE Firmware ***(Applies to both SDV Laptop and SDV Desktop)***	
Runtime Firmware	SDV2_VER_1.3.8
Embedded AA Firmware	AA 1.08
TOE Management Software ***(Applies to both SDV Laptop and SDV Desktop)***	
Administrative Software (SAU)	SAU 2.03
SDV Laptop Hardware	
SDV18A	VER A
SDV Desktop Hardware	
SDV201B	VER B

The SDV works independent of any Operating System (OS), with any standard ATA-5 HDD, and resides in the IDE channel, blocking and controlling all access to the HDD. The SDV works transparently to the Operating System and users.

The TOE encrypts the system HDD on a per partition basis using the FIPS PUB 140-2 Approved Rijndael algorithm with 128-bit keys in the Advanced Encryption Standard, FIPS PUB 197. For each HDD partition, a separate key is used for encryption. The SDV can encrypt a HDD with up to thirty-one partitions. One partition is reserved as a stealth partition that is used to hold management and configuration information; this stealth partition is unavailable to all users.

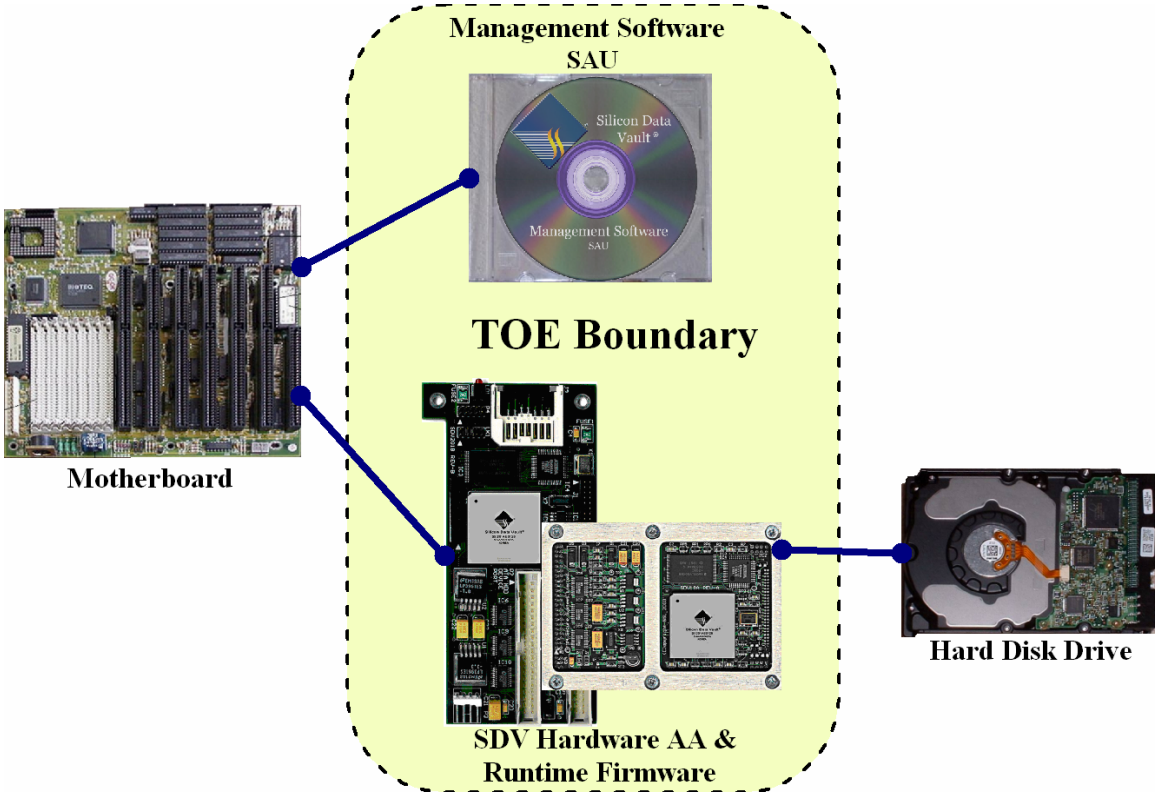
The TOE also provides read/write access control to all authorised users based on System Administrator defined permissions on a per partition basis. The System Administrator assigns each user a Username and Passphrase. A user may change their Passphrase after the System Administrator initial assignment. The System Administrator has read/write access to all partitions, with the exception of the stealth partition. Users (including the System Administrator) must successfully authenticate to the TOE in order to access partitions of the HDD based on their defined access permissions.

During the initial installation of the TOE hardware, the SDV is in a factory default insecure state, known as the INSTALL mode in the vendor documentation. This allows partitioning of the HDD and installation of the Operating System by the System Administrator. Secure installation of the TOE is not complete until the System Administrator account is created and the HDD has been encrypted. After HDD encryption, the TOE is in a secure state, known as the SECURE mode in the vendor documentation. After secure installation of the TOE, the only way to change the Operating System or repartition the HDD is to decrypt the HDD and uninitialise the TOE.

2.1.1 Physical Boundary

The physical boundary of the TOE encompasses the SDV hardware board and all components executed on that hardware, including firmware residing on the board and hardware components. Additionally, the SDV management software, stored and run from a bootable CD-ROM, is included in the TOE, this management software is known as the System Administrator Utility (SAU). When the CD-ROM containing the SAU is present, the administrator is required to login to the TOE prior to the loading of the Operating System. Should this CD not be present, the AA firmware provides this login functionality, also, prior to loading the Operating System. The HDD protected by the SDV is not included in the TOE boundary. Due to size constraints, the SDV Laptop ships with a Toshiba MK2004GAL 20GB HDD connected. This HDD is not part of the TOE and the System Administrator may substitute a different compatible HDD, if desired. The following diagram demonstrates the TOE and its relation to the host PC.

Figure 1 - Physical Boundary



2.1.2 Logical Boundary

The TOE logical boundary consists of the security features provided by the TOE. The TOE provides five security features: Identification and Authentication, Access Control, Data Protection, TOE Management, TOE Self Protection. The following is a brief description of the each security feature provided by the TOE.

A) Identification and Authentication – After initial secure installation, all user access to the TOE and the protected HDD can only proceed after the user has been both identified and authenticated by the TOE. Identification and Authentication is accomplished by the use of a Username/Passphrase combination. A SHA-1 hash of the Passphrase is compared with the stored known value. During the boot sequence of the PC, when the CD-ROM housing the TOE management software is not present, the PC's Bios attempts to boot from the HDD, the SDV mocks a HDD Master Boot Record (MBR) and executes the embedded AA firmware for user identification and authentication. Once authentication is complete, the user is given the opportunity to change their Passphrase, or load the Operating System. Once the user selects to load the Operating System, control is passed to the runtime firmware and the SDV operates transparently to the user. When booting the system with the TOE management software, the management software performs Identification and Authentication independent and prior to the loading of any Operating System. Then management of the TOE security functions can proceed.

B) Access Control – The TOE implements an Access Control mechanism based on users, their access permissions, and the partitions of the protected HDD. The user and access permissions are defined during user account creation. The System Administrator chooses which partitions of the HDD the user has access to and the level of access he/she has to that partition. The System Administrator may choose to grant the user read-only access to the partition or read/write access to the partition. If the System Administrator chooses to not assign a level of access for a particular partition to the user, the user will have no access to that partition (i.e., neither the Operating System nor the user have any knowledge that the partition even exists on the HDD). For example, if multiple users share a system, all users could have read-only access to the partition that houses the Operating System, and each user would have read/write access to a specific partition allocated for their own data.

C) Data Protection – The SDV provides a data protection feature that encrypts all data on the HDD. Each partition on the HDD is encrypted with its own key. All keys within the SDV are randomly generated using the PRNG in Appendix 3.1 of FIPS PUB 186-2. Each user is allocated access to the keys for partitions for which they have access. Keys are encrypted and stored along with authentication data on the stealth partition, with the exception of the key used to encrypt the stealth partition (it is stored within the SDV's FLASH). The partitions are encrypted using the algorithm in AES with 128-bit keys. The SDV is validated for conformance with the FIPS PUB 140-2 (Certificate pending).

D) TOE Management – The software held on the TOE management CD provides a GUI for the System Administrator to manage the TOE and the TOE's user security attributes. This code executes on the host machine's main processor and allows the administrator to log into the TOE prior to the loading and independent of any Operating System installed on the HDD. The TOE provides the ability for the System Administrator to create and delete user accounts. Each account is associated with a Username, a Passphrase, and a set of permissions detailing the partitions the user has access to and the level of access permitted. The management software allows the System Administrator to complete the TOE initialisation, including encrypting the entire HDD, each partition with its own key of the HDD. The TOE recognizes two roles, a (non-administrative) user and a System Administrator.

E) TOE Self Protection – The TOE is executed as three separate processes, each firmware/software component corresponding to its own process. The runtime firmware is executed on the SDV hardware. The SDV hardware provides the runtime firmware its own domain for execution that cannot be bypassed due to the design of the hardware. The SDV management software and embedded AA firmware execute independently and before the loading of any underlying Operating System. The Management software is located on a bootable CD-ROM and the embedded AA

firmware is located on the SDV's FLASH memory. Both execute on the host machine without any user intervention or host operating system, and allow no means whereby an operator can bypass the functionality once it has started execution. This implementation of the SDV management software and embedded AA firmware results in the remaining processes being non-bypassable and contained in a separate domain. As a whole, the TOE is non-bypassable and executes in its own domain.

2.2 Silicon Data Vault ® IT-Environment

The TOE operates independent of any Operating Systems and the OS chosen does not affect the performance of the TOE. However, there are several minimum requirements of the computer in which the TOE is operating, as follows.

A) The PC must be an IBM compatible PC.

B) The PC must have 16MB or more of RAM available.

C) The PC must have an ATA-5 compatible Hard Disk Drive.

D) The PC must use one of the following file systems:

1) FAT 16/FAT 32

2) NTFS

3) EXT 2/EXT 3

4) Reiser

E) The PC must have a CD-ROM reader.

The host computer in which the TOE resides may be network connected. If access permissions are granted by the IT environment administrator, then remote users on the network operate on behalf of the local user that has identified and authenticated during the initial boot sequence when accessing protected assets. Remote users accessing assets protected by the TOE have the same access rights as the identified and authenticated local user.

CHAPTER 3

3. Security Environment

3.1 Introduction

This chapter identifies the following:

A) Significant assumptions about the TOE's operational environment.

B) IT related threats to the organisation countered by the TOE.

C) Organisational security policies for the TOE as appropriate.

Using the above listing, this chapter identifies assumptions, identified A.XXXX, threats identified T.XXXX, and organisational security policies, identified P.XXXX.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

3.2.1 Personnel Assumptions

A.NO_EVIL	The System Administrator of the TOE will not attempt to attack or subvert the TOE and its policy.
A.POWEROFF	Each user will completely power-down the TOE (i.e., no soft-reset) after completion of their session with the TOE.
A.USERAUTH	The user will authenticate with credentials appropriate for the environment (networked, standalone) in which the TOE is installed.
A.ENVCONFIG	The IT environment administrator will configure environmental access controls in a manner appropriate for the environment (networked, standalone) in which the TOE is installed.

3.3 Threats

The TOE is a data protection device that protects all information on the protected HDD from disclosure and modification. The main underlying threat of the TOE is the access of this protected information by some entity that does not have the proper access rights. When securely installed, the TOE offers three layers of security to protect this information. First a user must be identified and authenticated before they can gain any access to the HDD. Following identification and authentication, the access control mechanism ensures that users gain access to only the partitions for which they have been granted access. The final layer of protection is the encryption of the HDD, which protects the information on the HDD from a direct access of the HDD (someone physically removes the HDD from the TOE's host PC and installs it on another host hoping to gain access to the information stored). The TOE is also designed to be an independent device, relying on no underlying operating system. This ensures the TOE, when securely installed, will execute as designed protecting it from interruption or logical bypass. To enforce the overall security goal of the TOE, the TOE addresses the threats

defined in section 3.3.1. Each threat is characterised in terms of threat agents, assets and means by which an attack is carried out.

Threat Agents are characterised as individuals and possibly computer applications working on behalf of individuals that carry out a threat. In the descriptions of threats the TOE counters below, the term *Operator* is used to cover these possible threat agents as some threats are likely to originate from multiple sources, i.e. an attacker or cracker, an inadvertent user, or an application executing on the host PC on the behalf of an individual. The *threat agents* addressed in this ST are assumed to have an attack potential of *low* with a *low* expertise of the TOE and *low* resources and motivation to attack the assets protected by the TOE.

Assets protected by the TOE include the components within the TOE boundary, and the information on the hard-drive connected to the TOE.

3.3.1 Threats Countered by the TOE

T.NOIDENT	An unidentified operator may gain access to the TOE through either malicious or accidental means.
T.UNAUTH	An unauthenticated operator may gain access to the TOE and/or the assets it protects through either malicious or accidental means.
T.NOACCESS	After authentication, an operator may gain access to partitions on the protected hard-drive for which they have not been granted access through either malicious or accidental means.
T.DISCLOSE	An individual, who has exploited an opportunity to gain physical access to the TOE and host PC, obtains stored information by directly accessing the HDD.
T.NOAVAIL	An operator may tamper or interfere with the security functions provided by the TOE by interrupting or bypassing the TOE during operation.
T.MANAGE	The System Administrator may perform unintended management actions if the TOE cannot be managed effectively through its management interfaces.

3.4 Organisational Security Policies

This Security Target contains no Organisational Security Policies

CHAPTER 4

4. Security Objectives

The Security Objectives identified in this Security Target ensure that all of the security threats listed in Chapter 3 have been countered and ensure that the assumptions and organisational security policies listed in Chapter 3 have been covered. The following conventions have been followed when identifying the Security Objectives.

Security Objectives of the TOE: O.XXXXX

Security Objectives of the Non-IT Environment: O.N.XXXXX

4.1 Security Objectives for the TOE

All of the objectives listed in this section ensure that all of the security threats have been countered and the organisational security policies have been covered. The security objectives for Silicon Data Vault ® are:

O. CONFIDENTIALITY	The TSF shall prevent unauthorised disclosure of information stored on the protected hard-drive.
O.AVAILABILITY	The TSF shall maintain a domain for its own execution that protects it from external interference, tampering and bypass of the TSF; while ensuring the services provided by the TSF are available.
O.I&A	The TSF shall ensure that only identified and authenticated operators gain access to the TOE, its assets and the assets protected by the TOE.
O.MANAGE	The TSF shall provide all the functions necessary to support the System Administrator in the management of TOE security.
O.ACCESS_CONTROL	The TSF shall only allow users access to assets for which they have been granted access, and the TSF shall deny all access to assets for which a user has not been allocated access.

4.2 Security Objectives for the non-IT Environment

All of the Non-IT Environment objectives listed in this section ensure that all of the assumptions of the TOE environment have been covered. The security objectives for the Non-IT Environment are:

O.N.PERSONNEL	The System Administrator of the TOE, a benevolent individual, will be a trustworthy individual.
O.N.POWEROFF	Users of the TOE will power-down the TOE after each session using the TOE.
O.N.USERUSE	The users of the TOE use the TOE in a manner consistent with the environment in which the TOE is installed (networked, standalone).

O.N.ADMINUSE	The administrator of the TOE and the environment will administrator the TOE and IT environment in a manner appropriate for the environment in which the TOE is installed (networked, standalone).

CHAPTER 5

5. IT Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC and explicitly stated functional components.

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 functional requirements identified as explicitly stated and the items within the functional requirements identified as operations that are TOE specific. The following table identifies the functional requirements of the TOE (both derived verbatim from Part 2 of the CC and explicitly stated).

Table 2 - TOE SFRs

SFR Component	SFR Name
TOE SFRs derived verbatim from Part 2 of the CC	
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1(a)	Cryptographic Operation
FCS_COP.1(b)	Cryptographic Operation
FDP_ACC.2	Complete Access Control
FIA_AFL.1	Authentication Failure Handling
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 Initialisation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_RVM.1	Non-Bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
Explicitly Stated TOE SFRs	
FDP_ACF.1-NIAP-0407	Security Attribute Based Access Control

5.1.1 Cryptographic Support (FCS)

5.1.1.1 FCS_CKM.1 Cryptographic Key Generation

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm FIPS PUB 140-2 Approved Random Number Generation and specified cryptographic key sizes 128-bits that meet the following: FIPS PUB 186-2 Appendix 3.1.

Dependencies: [FCS_CKM.2 Cryptographic Key Distribution

or

FCS_COP.1 Cryptographic Operation],

FCS_CKM.4 Cryptographic Key Destruction,

FMT_MSA.2 Secure Security Attributes.

Application Note: Conformance to FIPS PUB 140-2 and FIPS PUB 186-2 have been met through CMVP Validation Testing.

5.1.1.2 FCS_CKM.4 Cryptographic Key Destruction

Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method FIPS PUB 140-2 Approved Zeroization Technique that meets the following: FIPS PUB 140-2.

Dependencies: [FDP_ITC.1 Import of User Data Without Security Attributes

or

FCS_CKM.1 Cryptographic Key Generation],

FMT_MSA.2 Secure Security Attributes.

Application Note: Key Destruction is performed by an overwriting with zeroes; this conformance was tested during the CMVP Validation Testing.

5.1.1.3 FCS_COP.1(a) Cryptographic Operation

Hierarchical to: No other components.

FCS_COP.1.1(a) The TSF shall perform symmetric encryption/decryption in accordance with a specified cryptographic algorithm Rijndael algorithm and cryptographic key sizes 128-bits that meet the following: FIPS PUB 197 Advanced Encryption Standard in ECB Mode.

Dependencies: [FDP_ITC.1 Import of User Data Without Security Attributes

or

FCS_CKM.1 Cryptographic Key Generation],

FCS_CKM.4 Cryptographic Key Destruction,

FMT_MSA.2 Secure Security Attributes.

Application Note: AES conformance was tested during CMVP Validation Testing; CMVP AES Certificate Number 136 was issued.

5.1.1.4 FCS_COP.1(b) Cryptographic Operation

Hierarchical to: No other components.

FCS_COP.1.1(b) The TSF shall perform Secure Hashing in accordance with a specified cryptographic algorithm Secure Hash Algorithm (SHA-1) and cryptographic key sizes n/a that meet the following: FIPS PUB 180-2 Secure Hash Standard.

Dependencies: [FDP_ITC.1 Import of User Data Without Security Attributes

or

FCS_CKM.1 Cryptographic Key Generation],

FCS_CKM.4 Cryptographic Key Destruction,

FMT_MSA.2 Secure Security Attributes.

Application Note: SHA-1 conformance was tested during CMVP Validation Testing; CMVP SHS Certificate Number 219 was issued.

5.1.2 User Data Protection (FDP)

5.1.2.1 FDP_ACC.2 Complete Access Control

Hierarchical to: FDP_ACC.1 Subset Access Control.

FDP_ACC.2.1 The TSF shall enforce the TFAB Policy on Subjects: All Users, Objects: Partitions on the Protected HDD and all operations among subjects and objects covered by the SFP.

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

Dependencies: FDP_ACF.1 Security Attribute Based Access Control.

5.1.2.2 FDP_ACF.1-NIAP-0407 Security Attribute Based Access Control

Hierarchical to: No other components.

FDP_ACF.1.1-NIAP-0407 The TSF shall enforce the TFAB Policy to objects based on the following: Subjects: All Users,

Objects: Partitions,

Subject Attributes: Partition Access Permissions,

Object Attributes: No SFP-relevant security attributes.

FDP_ACF.1.2-NIAP-0407 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: Each User will have the Partition Access Permissions specified by the System Administrator at the time of User account creation. The access rights include: read-only partition access, read/write partition access, and no partition access.

FDP_ACF.1.3-NIAP-0407 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *System Administrator has read/write partition access to all partitions with the exception of the "stealth partition"*.

FDP_ACF.1.4-NIAP-0407 The TSF shall explicitly deny access of subjects to objects based on the following rules: *All Users have no partition access to the "stealth partition"*.

Dependencies: FDP_ACC.1 Subset Access Control,

FMT_MSA.3 Static Attribute Initialisation.

5.1.3 Identification and Authentication (FIA)

5.1.3.1 FIA_AFL.1 Authentication Failure Handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when *three* unsuccessful authentication attempts occur related to power-on of the TOE.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall deny all authentication attempts until a power-cycle of the TOE occurs.

Dependencies: FIA_UAU.1 Timing of Authentication.

5.1.3.2 FIA_SOS.1 Verification of Secrets

Hierarchical to: No other components.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that **Passphrases** meet a length of six to fifty-four (inclusive) characters coming from a character set with a cardinality of ninety-three.

Dependencies: No dependencies.

5.1.3.3 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.

Application Note: Remote users assume the access rights of the identified and authenticated local user when remotely accessing protected assets.

5.1.3.4 FIA_UAU.7 Protected Authentication Feedback

Hierarchical to: No other components.

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

Dependencies: FIA_UAU.1 Timing of Authentication.

5.1.3.5 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.

Application Note: Remote users assume the access rights of the identified and authenticated local user when remotely accessing protected assets.

5.1.4 Security Management (FMT)

5.1.4.1 FMT_MSA.1 Management of Security Attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the TFAB Policy to restrict the ability to *change_default, delete* the security attributes Partition Access Permissions to System Administrator.

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.

5.1.4.2 FMT_MSA.3 Static Attribute Initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the TFAB 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 System Administrator to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of Security Attributes,

FMT_SMR.1 Security Roles.

5.1.4.3 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: create/delete Users, set User Partition Access Permissions during User account creation, and encrypt the HDD.

Dependencies: No dependencies.

5.1.4.4 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles System Administrator and User.

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

Dependencies: FIA_UID.1 Timing of Identification.

Application Note: The System Administrator is a User with administrative permissions.

5.1.5 Protection of the TSF (FPT)

5.1.5.1 FPT_RVM.1 Non-Bypassability of the TSP

Hierarchical to: No other components.

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.

Dependencies: No dependencies.

5.1.5.2 FPT_SEP.1 TSF Domain Separation

Hierarchical to: No other components.

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

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

Dependencies: No dependencies.

5.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2. These requirements are summarised in Table 1.

Table 3 - 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

Assurance Class	Component ID	Component Title
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

5.3 Security Requirements for the IT Environment

There are no Security Functional Requirements for the IT Environment.

5.4 Strength of Function Claims

The only probabilistic or permutational mechanism in the TOE is the Passphrase 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.

5.5 Strength of Function Rationale

The claimed minimum strength of function is SOF-basic. All user authentication requirements in FIA_SOS.1 and FIA_UAU.1 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 Passphrase length.

CHAPTER 6

6. TOE Summary Specification

6.1 TOE Security Functions

The security functions implemented by the TOE are:

Identification and Authentication (I&A)

After secure installation, the TOE requires all entities attempting to access the TOE or TOE protected assets (i.e. the protected HDD) to be identified and authenticated before any other actions (**FIA_UID.2.1, FIA_UAU.2.1**). Users are authenticated with a Passphrase with a length of six to fifty-four characters (inclusive) coming from a character set with a cardinality of ninety-three (**FIA_SOS.1.1**). This Passphrase is hashed using the FIPS PUB 140-2 Approved SHA-1 (**FCS_COP.1.1(b)**). The calculated message digest is compared with the known correct value; if they match, the user is authenticated else authentication fails. During Passphrase entry, asterisks are used to obscure the entered text (**FIA_UAU.7.1**). After three unsuccessful authentication attempts after power-on of the TOE, the TOE denies all users from authenticating with the TOE (**FIA_AFL.1.1, FIA_AFL.1.2**). A power-cycle of the TOE is required before authentication can be accomplished (**FIA_AFL.1.2**).

TOE SFRs met by the I&A SF: FIA_UAU.2, FIA_UID.2, FIA_UAU.7, FIA_SOS.1, FCS_COP.1(b), FIA_AFL.1

Access Control

The TOE implements an access control policy. This policy controls all actions between the Users of the TOE and the partitions of the protected HDD based on Partition Access Permissions assigned to the User (**FDP_ACC.2.1, FDP_ACF.1.1-NIAP-0407**). No operations are permitted that are not covered by the access control policy (**FDP_ACC.2.2**). At the time of User account creation, the System Administrator defines the Partition Access Permissions for that User. These permissions define the level of access the User has for each partition. The access levels available are: read-only partition access, read/write partition access, and no partition access (**FDP_ACF.1.2-NIAP-0407**). With the exception of the stealth partition, the System Administrator has read/write partition access to all partitions (**FDP_ACF.1.3-NIAP-0407**). All Users have no partition access to the stealth partition (**FDP_ACF.1.4-NIAP-0407**).

TOE SFRs met by the Access Control SF: FDP_ACC.2, FDP_ACF.1-NIAP-0407

Data Protection

The Cryptographic Module within the TOE has been tested for compliance with FIPS PUB 140-2 and has received FIPS PUB 140-2 Certificate #477. The TOE encrypts all raw data on the protected HDD during HDD writes and it decrypts all raw data on the protected HDD during HDD reads using the FIPS PUB 140-2 Approved Rijndael Algorithm from the Advanced Encryption Standard using 128-bit keys (**FCS_COP.1.1(a)**). Each partition has its own key. The key for the stealth partition is known as the configuration key, all other partition keys are simply known as partition keys. The partition keys are retained on the stealth partition. All keys within the TOE are generated using the FIPS PUB 140-2 Approved RNG in Appendix 3.1 of FIPS PUB

186-2, the Digital Signature Standard (**FCS_CKM.1.1**). If the TOE is securely uninstalled (i.e. uninitialised and then removed), all Cryptographic Keys are destroyed (zeroized) using FIPS PUB 140-2 Approved Zeroization Techniques; the keys are overwritten with a stream of zeroes (**FCS_CKM.4.1**).

TOE SFRs met by the Data Protection SF: FCS_CKM.1, FCS_CKM.4, FCS_COP.1(a)

TOE Management

The TOE provides a suite of management utilities for the secure management of the TOE. Two roles are supported by the TOE, that of System Administrator and User (**FMT_SMR.1.1**). The System Administrator is a User with administrative permissions. During secure installation of the TOE, a User is associated with the System Administrator role. All subsequent Users created are associated with the User role (**FMT_SMR.1.2**). The System Administrator is the only role permitted the capability to securely manage the TOE using the management utilities. The TOE provides the System Administrator with the ability to encrypt the protected HDD (part of secure installation), create Users, assign the User's Partition Access Permissions, and delete Users (**FMT_SMF.1.1**). During User account creation, the System Administrator can change the default Partition Access Permissions for Users (**FMT_MSA.1.1**). The System Administrator can delete a User account and thereby delete the Partition Access Permissions for that User (**FMT_MSA.1.1**). By default, the TOE provides new User accounts created with no partition access (**FMT_MSA.3.1**). Only the System Administrator can override the default values with either read-only exclusive-or read/write partition access (**FMT_MSA.3.2**). The functionality described provides the System Administrator with the ability to securely manage the security functions of the TOE.

TOE SFRs met by the TOE Management SF: FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1

TOE Self Protection

The TOE implements two security mechanisms to ensure that the security functions cannot be bypassed or be tampered with. The TOE consists of three main executable components, the management software, the embedded AA firmware, and the run-time firmware. The management software is executed from a bootable CD-ROM that cannot be bypassed (**FPT_RVM.1.1**). Once initialised the management software immediately performs identification and authentication ensuring that the TSF cannot be bypassed (**FPT_RVM.1.1**). When the management software CD-ROM is not present in PC, the embedded AA portion of the TOE acts as the MBR of the protected HDD and prevents the access of the protected HDD. The embedded AA portion of the TOE performs user identification and authentication before any other action ensuring the TSF cannot be bypassed (**FPT_RVM.1.1**). The run-time firmware executes the access control and cryptographic mechanisms automatically on the TOE's hardware and is initialised by the embedded AA firmware following identification and authentication, ensuring that the TSF cannot be bypassed (**FPT_RVM.1.1**). The management software and the embedded AA firmware execute without any underlying operating system, providing their own domain for execution (**FPT_SEP.1.1, FTP_SEP.1.2**). The run-time firmware is

executed on the TOE's hardware that is physically distinct from the host PC (**FPT_SEP.1.1, FTP_SEP.1.2**).

TOE SFRs met by the TOE Self Protection SF: FPT_RVM.1, FPT_SEP.1

6.2 TOE Security Function Rationale

Table 2 demonstrates the correspondence between the security functional requirements identified in Sections 5.1 and the TOE security functions identified in Section 6.1.

Table 4 - Mappings Between TOE Security Functional Requirements and TOE Security Functions

	I&A	Access Control	Data Protection	TOE Management	TOE Self Protection
FCS_CKM.1			X		
FCS_CKM.4			X		
FCS_COP.1(a)			X		
FCS_COP.1(b)	X				
FDP_ACC.2		X			
FDP_ACF.1-NIAP-0407		X			
FIA_AFL.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_SMF.1				X	
FMT_SMR.1				X	
FPT_RVM.1					X
FPT_SEP.1					X

As shown in the Security Function definitions and the previous SFR to SF mapping table, all TOE SFRs mapped to the identified Security Functions are fully met by the Security

Function. This is evidenced by the characteristics of the Security Functions described in section 6.1.

6.3 Assurance Measures

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.

The assurance measures provided by the TOE satisfy all of the assurance requirements listed in the following table, which provides a reference between each TOE assurance requirement and the related vendor documentation that satisfies each requirement.

Table 5 - Assurance Measures and Rationale

Component ID	Assurance Measures	Rationale
ACM_CAP.2	Developer Configuration Management Documentation	This documentation describes the configuration management system of all the components of the TOE. Also included in the documentation is a configuration list of all the items that comprise the TOE.
ADO_DEL.1	Developer Delivery Documentation	This document includes descriptions of the process used to create distribution copies of the TOE and the procedures used to ensure consistent delivery of the TOE.
ADO_IGS.1	Developer Secure Installation and Start-up Documentation	These documents describe the procedures necessary for secure installation, generation, and start-up of the TOE.
ADV_FSP.1	Developer Functional Specification	These documents provide the purpose and methods of use for all external TSF interfaces and completely represent the TSF.
ADV_HLD.1	Developer High-Level Design	These documents describe the high level design. They contain a representation of the TSF in terms of subsystems, identifying the TSP-enforcing subsystems, and describe the

Component ID	Assurance Measures	Rationale
		security functions. All subsystem interfaces are identified and the externally visible ones are noted. The purpose and method of use of all interfaces to the TSF subsystems are described.
ADV_RCR.1	Developer Development Correspondence Documentation	The correspondence between the TOE security functions and the functional specification and the correspondence between the functional specification and the high-level design subsystems is described in these documents.
AGD_ADM.1	Administrative Guidance Documentation	Guidance to administrators is effectively supported by the listed documentation for this requirement.
AGD_USR.1	User Guidance Documentation	Guidance to non-administrative users is effectively supported by the listed documentation for this requirement.
ATE_COV.1	Developer Test Documentation	These documents describe the functional and penetration tests performed and their results.
ATE_FUN.1	Developer Test Documentation	These documents describe the functional and penetration tests performed and their results.
ATE_IND.2	Developer Test Documentation Evaluation Lab Independent Testing	These documents describe the functional and penetration tests performed and their results.
AVA_SOF.1	Developer Strength of Function Documentation	These documents include a strength of function analysis to support the SOF-basic claim.
AVA_VLA.1	Developer Vulnerability Analysis Evaluation Lab Independent Vulnerability Assessment	These documents describe the vulnerability analysis performed and the results of the analysis.

6.4 Appropriate Strength of Function Claim

The authentication mechanism includes a Passphrase-based authentication feature that is probabilistic. FIA_SOS.1 and FIA_UAU.2 are the only TOE security functional requirements that depend on this permutational function. The I&A Security Function is the only security function that depends on this permutational function.

The rationale for choosing SOF-basic overall is based on the low attack potential of the threats identified in this ST. The security objectives provide probabilistic security mechanisms and the strength of function claim is satisfied by the Passphrase management features provided by the TOE.

CHAPTER 7

7. Protection Profile Claims

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

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

8.1 Security Objectives Rationale

Table 4 demonstrates the correspondence between the security objectives listed in Sections 4.1 and 4.2 to the assumptions, threats and policies identified in Sections 3.2, 3.3 and 3.4.

Table 6 - Mappings Between Assumptions, Threats, and Policies and Security Objectives

	T.NOIDENT	T.UNAUTH	T.NOACCESS	T.DISCLOSE	T.NOAVAIL	T.MANAGE	A.NO_EVIL	A.POWEROFF	A.USERAUTH	A.ENVCONFIG
O. CONFIDENTIALITY				X						
O.AVAILABILITY					X					
O.I&A	X	X								
O.MANAGE						X				
O.ACCESS_CONTROL			X							
O.N.PERSONNEL							X			
O.N.POWEROFF								X		
O.N.USERUSE									X	
O.N.ADMINUSE										X

8.1.1 Rationale for TOE Security Objectives

T.NOIDENT is countered by O.I&A. O.I&A counters T.NOINDENT by ensuring that prior to any entity gaining access to the TOE that the TSF identifies the entity. By accomplishing this objective the TOE removes the possibility of T.NOINDENT occurring.

T.UNAUTH is countered by O.I&A. O.I&A counters T.UNAUTH by ensuring that prior to any entity gaining access to the TOE or protected assets of the TOE that the TSF authenticates the entity. By accomplishing this objective the TOE removes the possibility of T.UNAUTH occurring.

T.NOACCESS is countered by O.ACCESS_CONTROL. O.ACCESS_CONTROL counters T.NOACCESS by ensuring that access to information stored on the partitions of

the protected HDD is only given to users granted the appropriate level of access. By accomplishing this objective the TOE removes the possibility of T.NOACCESS occurring.

T.DISCLOSE is countered by O.CONFIDENTIALITY. O.CONFIDENTIALITY counters T.DISCLOSE by ensuring that all information stored on the protected HDD is kept in an unreadable form. All raw data is stored on the HDD in ciphertext. By accomplishing this objective the TOE diminishes the possibility that T.DISCLOSE will be successful, requiring greater expertise and assets than are available to the threat agent (low expertise and low resources).

T.NOAVAIL is countered by O.AVAILABILITY. O.AVAILABILITY counters T.NOAVAIL by ensuring that the TOE functions are always performed, in their own domain, and that the TOE is (logically) non-bypassable. By accomplishing this objective the TOE removes the possibility of T.NOAVAIL occurring.

T.MANAGE is countered by O.MANAGE. O.MANAGE counters T.MANAGE by the TOE providing a set of management functions that provide the System Administrator with the utilities to effectively manage the TOE security. By accomplishing this objective the TOE removes the possibility of T.MANAGE occurring.

8.1.2 Rationale for non-IT Environment Security Objectives

A.NO_EVIL is covered by O.N.PERSONNEL. O.N.PERSONNEL covers A.NO_EVIL by providing there will be no evil System Administrator.

A.POWEROFF is covered by O.N.POWEROFF. O.N.POWEROFF covers A.POWEROFF by providing that the users of the TOE will power-down the TOE after their completed session.

A.USERAUTH is covered by O.N.USERUSE. O.N.USERUSE covers A.USERAUTH by providing that the users of the TOE will act in a manner appropriate for the environment the TOE is installed within. This includes understanding the network access rights of remote users and authenticating using the appropriate credentials, if appropriate.

A.ENVCONFIG is covered by O.N.ADMINUSE. O.N.ADMINUSE covers A.ENVCONFIG by providing that the environment in which the TOE is installed is administered in an appropriate manner. This includes crafting any remote access controls in a manner consistent with the protection provided by the TOE, if appropriate.

8.2 Security Requirements Rationale

8.2.1 Security Functional Requirements Mutually Supportive Whole Rationale

The set of IT Security Requirements work together to form a mutually supportive whole. The identified TOE SFRs work together to ensure that all Security Objectives of the TOE are met. Additionally, the identified TOE SFRs together implemented the Security Functions, identified in Chapter 6.

8.2.2 Security Functional Requirements Rationale for the TOE

Table 5 demonstrates the correspondence between the security objectives listed in Sections 4.1 to the security functional requirements identified in Sections 5.1.

Table 7 - Mappings Between TOE Security Objectives and TOE Security Functional Requirements

	O.CONFIDENTIALITY	O.AVAILABLITY	O.I&A	O.MANAGE	O.ACCESS_CONTROL
FCS_CKM.1	X				
FCS_CKM.4	X				
FCS_COP.1(a)	X				
FCS_COP.1(b)			X		
FDP_ACC.2					X
FDP_ACF.1-NIAP-0407					X
FIA_AFL.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_SMF.1				X	
FMT_SMR.1				X	
FPT_RVM.1		X			
FPT_SEP.1		X			

FCS_CKM.1, FCS_CKM.4, and FCS_COP.1 cumulatively enforce O.CONFIDENTIALITY. These SFRs provide the encryption requirements of information stored on the TOE protected HDD for the TOE. FCS_CKM.1, and FCS_CKM.4 specify the FIPS PUB 140-2 Approved cryptographic key generation and storage methods implemented by the TSF. FCS_COP.1 specifies the Rinjdael Algorithm in the Advanced Encryption Standard as the symmetric encryption algorithm supported by the TSF. By requiring these characteristics of the TOE, O.CONFIDENTIALITY is enforced.

FPT_RVM.1 and FPT_SEP.1 cumulatively enforce O.AVAILABLITY. These SFRs provide the self-protection requirements of the TOE. Specifically, FPT_RVM.1 specifies that the security functions provided by the TSF will be invoked prior to proceeding with any actions on the TOE or the TOE protected HDD. FPT_SEP.1 specifies that a separate security domain for the TOE be maintained. By requiring these characteristics of the TOE, O.AVALABILITY is enforced.

FCS_COP.1(b), FIA_AFL.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.7, and FIA_UID.2 cumulatively enforce O.I&A. These SFRs provide the identification and authentication requirements of the TOE. FCS_COP.1(b) specify that a FIPS 140-2 Approved hashing method in a FIPS 140-2 Validated Cryptographic Module be used to hash the user Passphrase. FIA_AFL.1 specifies how the TOE handles unsuccessful authentication attempts. FIA_SOS.1 specifies the minimum requirements of the Passphrases used in user authentication. FIA_UAU.2 and FIA_UID.2 specify that users of the TOE must be successfully authenticated and identified prior to performing any actions that involve the security functions of the TSF. FIA_UAU.7 specifies that only asterisks be provided as feed back during authentication attempts. By requiring these characteristics of the TOE, O.I&A is enforced.

FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, and FMT_SMR.1 cumulatively enforce O.MANAGE. The SFRs provide the security management requirements of the TOE. FMT_MSA.1 specifies actions available to the System Administrator regarding security attributes provided by the TOE. FMT_MSA.3 specifies that default values of security attributes provided by the TOE are restrictive and that the System Administrator is the only role that has the ability to change those defaults. FMT_SMF.1 specifies the security functions provided by the TOE. FMT_SMR.1 identifies the roles provided by the TOE. By requiring these characteristics of the TOE, O.MANAGE is enforced.

FDP_ACC.2 and FDP_ACF.1-NIAP-0407 cumulatively enforce O.ACCESS_CONTROL. The SFRs provide the access control policy requirements enforced by the TOE. Specifically, FDP_ACC.2 specifies the subjects and objects that the access control policy of the TOE is applicable to. FDP_ACF.1-NIAP-0407 specifies the access control rules associated with the access control of the TOE. By requiring these characteristics of the TOE, O.ACCESS_CONTROL is enforced.

8.2.3 Security Functional Requirements Rationale for the IT Environment

This ST contains no Security Functional Requirements for the IT Environment.

8.2.4 Security Assurance Requirements Rationale

The rationale for the Security Assurance Requirements is defined in Chapter 6, Section 6.3.

8.2.5 Security Functional Requirements Dependencies Not Met Rationale

All of the CC provided SFRs in the FCS family depend on FMT_MSA.2 Secure Security Attributes. Once the TOE has been securely installed, the cryptographic functions are performed automatically, requiring no input by the User or System Administrator. The cryptographic functions require no Security Attributes outside of the secure values automatically generated by the functions themselves (cryptographic keys), which have been validated by the CMVP.

FDP_ACC.2 has a dependency on FDP_ACF.1. This dependency is met by the explicitly stated requirement FDP_ACF.1-NIAP-0407 (a NIAP Interpretation).

FIA_AFL.1 and FIA_UAU.7 have a dependency on FIA_UAU.1. This dependency is met by the hierarchical requirement FIA_UAU.2.

FIA_UAU.2 and FMT_SMR.1 have a dependency on FIA_UID.1. This dependency is met by the hierarchical requirement FIA_UID.2.

FDP_ACF.1-NIAP-0407 and FMT_MSA.1 have a dependency on FDP_ACC.1. This dependency is met by the hierarchical requirement FDP_ACC.2.

8.2.6 Explicit Security Functional Requirements Rationale

FDP_ACF.1-NIAP-0407 has been included as a result of NIAP Interpretation #0407.

8.3 TOE Summary Specification Rationale

The rationale for the TOE Summary Specification is defined in Chapter 6, Section 6.2.

8.4 PP Claims Rationale

The rationale for the Protection Profile conformance claims is defined in Chapter 7, Section 7.4 Protection Profile Rationale.

CHAPTER 9

9. Glossary of Terms

The following is a list of terms and associated definitions used in this ST:

Ciphertext – Raw data that has been encrypted.

Information – The meaning of data, what a person interprets data to mean.

Operator – An individual or software application acting on an individual's behave.

Passphrase - A string of words and characters that a TOE user uses to authenticate him/herself.

Raw Data – The raw data (bits) on the HDD.

Stealth Partition – The special partition on the HDD that the SDV uses for configuration data.

TFAB Policy – Access Control Policy enforced by the TOE.

CHAPTER 10

10. References

The following documents and sources are referenced or were used in the authoring of this Security Target:

1. Common Criteria for Information Technology Security Evaluation, CCIMB-2004-01-001, CCIMB-2004-01-002, CCIMB-2004-01-003, Version 2.2, January 2004

2. Common Methodology for Information Technology Security Evaluation, Version 2.2, January 2004

3. Federal Information Processing Standard Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules, with Change Notices December 03, 2002

4. Federal Information Processing Standard Publication (FIPS PUB) 180-2, Secure Hash Standard, with Change Notice 1 February 25, 2004

5. Federal Information Processing Standard Publication (FIPS PUB) 186-2, Digital Signature Standard, with Change Notice 1 October 5, 2001

6. Federal Information Processing Standard Publication (FIPS PUB) 197, Advanced Encryption Standard, November 26, 2001

7. Gollman, Dieter, Computer Security, John Wiley & Sons Ltd, New York, ©1999. ISBN: 0-471-97844-2

8. ISO/IEC JTC 1/SC27, Guide for the Production of PPs and STs, Version 0.9