Silicon Data Vault® (SDV®)

SDV201B ♦ SDV18A

FIPS 140-2 Non-Proprietary Security Policy

Level 1 Validation

Document Version 2.4
October 2004

Document Revision History		
SSL FIPS 001 Appendix B, 11/19/2003 initial release SSL FIPS SP 001, 1/28/2004, Revision 1.0 SSL FIPS SP 001, 4/28/2004, Revision 2.3	Contact: Marilyn Windsor Checked: Approved: File Name: FIPS SDV SP_2.3.doc 10/07/04~~10/5/2004~~ Title: **FIPS 140-2 Security Policy Silicon Data Vault® SDV 201B Rev B, SDV 18A, & SKV18A**	**Secure Systems Limited** **Level 1, 80 Hasler Road** **Osborne Park, Western Australia 6017** **Tel: + 61 8 9292 8333** **Fax: + 61 8 9202 8334**

Table of Contents

1. Introduction 4

1.1 Purpose 4

1.2 References 4

1.3 Document Organisation 4

1.4 Intended FIPS 140-2 Security Levels 5

2. Silicon Data Vault® Description 6

2.1 Overview 6

2.1.1 SDV® Hardware, Firmware and Software Version Numbers 7

2.1.2 SDV201B Module 7

2.1.3 SDV18A Module 7

2.1.4 SDV®2_AES_V65 FPGA Logic 7

2.1.5 SDV® Firmware, SDV2_VER_1.3.4 8

2.1.6 SDV® Authentication Service 8

2.2 Cryptographic Boundary 9

2.3 SDV® Interfaces 10

3. SDV® Access Control Policy 11

3.1 Roles Supported 11

3.1.1 Super User Role 11

3.1.2 User Role 11

3.2 Authentication Required 11

3.3 Services Provided by the SDV® 12

3.3.1 SDV® Initialization 12

3.3.2 Backup of Selected Partitions to Stealth Partition 12

3.3.3 Recovery/Restore Functions 12

3.3.4 Creation of User Profile(s) 13

3.3.5 Event Log Viewing 13

3.3.6 Updating the SDV® RTC (to the computer RTC) 13

3.3.7 Authenticate User/Super User 13

3.3.8 Encryption of Data 13

3.3.9 Decryption of Data 13

3.3.10 Hashing 13

3.3.11 Zeroization .... 14~~13~~

3.3.12 Show Status 14

3.3.13 Power-On Self Tests 14

3.3.14 Conditional Tests 14

3.4 Services Allocated to Roles 14

3.5 Access Rights within Services .... 16~~15~~

4. SDV® Operation .... 17~~16~~

5. Physical Security Policy .... 18~~17~~

6. Operating Environment .... 18~~17~~

7. Key and CSP Generation .... **18~~17~~**

8. FCC EMI/EMC Requirements .... **18~~17~~**

9. Self Tests .... **20~~18~~**

10. Mitigation of Other Attacks Policy .... **20~~18~~**

10.1 Dictionary Attack .... 20~~18~~

11. Glossary .... **21~~19~~**

List of Figures

Figure 1. SDV® Desktop and Laptop Models 6
Figure 2. SDV® Cryptographic Boundary .... 10~~9~~
Figure 3. SDV® INSTALL Mode Illustrated .... 17~~16~~
Figure 4. SDV® SECURE (FIPS 140-2-Approved) Mode Illustrated .... 17~~16~~

List of Tables

Table 1. SDV® Security Levels 5
Table 2. SDV® Hardware, Firmware and Software Version Numbers 7
Table 3. SDV® FIPS Interfaces 10
Table 4. SDV® Physical Interfaces 10
Table 5. SDV® Role/Authentication Policy 11
Table 6. SDV® Services Allocated to Roles 14
Table 7. SDV® Access Right within Services .... 16~~15~~
Table 8. SDV® Self-Tests .... 20~~18~~
Table 9. SDV® Security Policy Glossary .... 21~~19~~

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Silicon Data Vault® (SDV®)resident in SDV® desktop model SDV201B, Revision B, and laptop model SDV18A, Revision A from the Secure Systems Limited's security solutions. It describes how the SDV® meets the security requirements of FIPS 140-2 and how to operate the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – Security Requirements for Cryptographic Modules) details the US and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standards and validation program is available on the NIST website at www.nist.gov/cmvp.

Throughout this document, the cryptographic module is referred to as the Silicon Data Vault®, 'SDV®', and 'the module'.

1.2 References

This document deals only with the operations and capabilities of the Silicon Data Vault® in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available from the following sources:

- Federal Information Processing Standard Publication 140-2 "Security Requirements for Cryptographic Modules," (Supercedes FIPS Publication 140-1, 11 January 1994

- Federal Information Processing Standard Publication 180-1 "Secure Hash Standard (SHS)"

- Federal Information Processing Standard Publication 186-2 "Digital Signature Standard (DSS)" Appendix 3.1 Pseudo Random Number Generator (PRNG)

- Federal Information Processing Standard Publication 197 "Advanced Encryption Standard (AES)"

1.3 Document Organisation

The Security Policy is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains a Vendor Evidence document and other supporting documentation as additional appendices.

This Security Policy for the SDV® and the other validation submission documentation were produced by Secure Systems Limited (SSL) and, with the exception of this non-proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to SSL and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact SSL.

1.4 Intended FIPS 140-2 Security Levels

The SDV® is validated to meet FIPS 140-2 security requirements for the levels shown in the following table. The overall multichip embedded module is validated for Security Level 1.

Table 1. SDV® Security Levels

Area	FIPS 140-2 Intended Security Level
Cryptographic Module Specification	Level 1
Cryptographic Module Ports and Interfaces	Level 1
Roles, Services, and Authentication	Level 2
Finite State Model	Level 1
Physical Security	Level 1
Operational Environment	N/A
Cryptographic Key Management	Level 1
EMI/EMC	Level 3
Power-up Self Tests	Level 1
Design Assurance	Level 3
Mitigation of Other Attacks	Level 1

2. Silicon Data Vault® Description

2.1 Overview

The Silicon Data Vault® (SDV®) is a hardware-based security device designed to prohibit unauthorized computer access through strong user authentication while encryption and a sophisticated key management scheme enforce data protection.

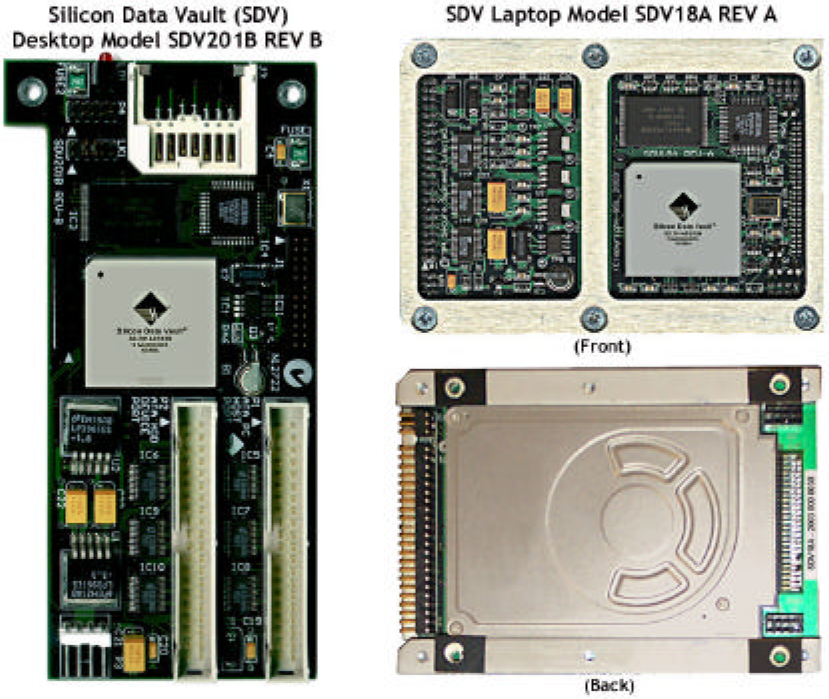

Figure 1. SDV® Desktop and Laptop Models

It offers an alternative to software based security methods and includes the following features:

- Encryption using 128-bit AES for disk reads and writes
- Algorithms:
  FIPS Approved: AES (Cert. #136), SHA-1 (Cert. #219)
  Random Number Generation: FIPS 186-2 A3.1 PRNG
  Non-FIPS: CRC-32
- One factor authentication (passphrase)
- Backup and recovery options
- Unlimited users
- Up to 31 partitions
- Un-install feature
- Easy user management
- All PIO, Multiword PIO and DMA modes
- 48-bit LBA (Hard disk > 137GB)
- Log archiving

The SDV® does not support multiple concurrent operators, remote administration, biometrics, or provide file level access control.

2.1.1 SDV® Hardware, Firmware and Software Version Numbers

Table 1 defines the SDV® hardware and firmware validated to FIPS 140-2. The software version for the System Administrative Utility (SAU) has also been included, is required for the Crypto-Officer to administer and setup the module, but not part of the cryptographic module.

Table 2. SDV® Hardware, Firmware and Software Version Numbers

Component	Model/Version Number
Hardware (Desktop)	SDV201B VER B
Hardware (Laptop)	SDV18A VER A
FPGA Logic	SDV2_AES_V65
Runtime Firmware	SDV2_VER_1.3.4
Embedded AA Firmware	AA 1.07
Administration Software (SAU)	SAU 1.05.1 (outside module boundary)

2.1.2 SDV201B Module

The SDV201B module consists of a multilayer printed circuit board assembly on which all components are mounted directly to both sides of the board. The board is of production grade printed circuit card quality; the chips feature a standard passivation coating. A supporting bracket allows the unit to be installed within a standard desktop personal computer enclosure. The SDV201B printed circuit board contains a single Altera FPGA device and several support peripherals. Access to all input and output signals are provided by connectors mounted directly on the board.

2.1.3 SDV18A Module

The SDV18A module consists a multilayer printed circuit board assembly, on which all components are mounted directly, including support brackets and a 1.8 inch HDD. The board is of production grade printed circuit card quality; the chips feature a standard passivation coating. The supporting brackets allow the unit to be installed within a standard notebook personal computer in place of the existing 2.5 inch HDD. Installation of the SDV18A should be in accordance with the computer manufacturers recommendations for replacement of the original HDD.

The SDV18A printed circuit board contains a single Altera FPGA device and several support peripherals. Access to all input and output signals are provided by connectors mounted directly on the board.

2.1.4 SDV®2_AES_V65 FPGA Logic

All major functions of the SDV201B and SDV18A are implemented in hardware within a single FPGA device. The SDV2_AES_V65 logic utilises approximately 90% of the hardware resources available within the FPGA device. The major blocks implemented within the design are a 32 Bit supervisory microprocessor, an ATA compatible device interface, an ATA compatible host interface, and a128 Bit AES encryption. The FPGA Logic firmware is loaded from Flash memory to configure and initialize the FPGA when power is first applied to the SDV.

2.1.5 SDV® Firmware, SDV2_VER_1.3.4

SDV2_VER_1.3.4 defines the operation of the system at run time. This firmware is responsible for supervising all communications on the IDE channel with the help of custom hardware (FPGA). It manages all SDV® resources including the Real Time Clock (RTC), flash read/writes and serial ports for debugging. SDV2_VER_1.3.4 operates in two modes: INSTALL and SECURE (FIPS 140-2 Approved).

2.1.6 SDV® Authentication Service

The SDV® authentication service is comprised of two embedded 80x86 codes to implement the user interface: the System Administration Utility (SAU), SAU 1.05.1, and the Authentication Application (AA), AA1.07. The AA loads directly from the SDV® and the SAU loads from a CD. They each run on an IBM-compatible PC; the ultimate goal being for either application to have the capability to run on all brands and models of IBM-compatible computers.

2.1.6.1 SAU 1.05.1

The SAU software (on external CD) provides the Super User a graphical interface with the means to do the following administrative tasks:

- Initialize a new SDV®
  - Synchronize SDV® RTC
  - Configure Stealth Partition
  - Record Replacement SDV® Information
  - Create Super User Account
- Replace an SDV® (Recover SDV® Configuration).
- Configure normal user profiles
- Encrypt disk partitions
- Provide backup and recovery services
- View Events log information
- Reset RTC
- Uninstall SDV

Note: The SAU software is outside of the Cryptographic Module’s boundary but is necessary for the administration and setup of the module.

2.1.6.2 AA1.07

The embedded AA firmware is located on the SDV®. During boot, the SDV2_VER_1.3.4 intercepts the MBR request and loads the SSL MBR and AA1.07 to the host computer for execution. The AA takes control of all host computer resources before any intervention with the HDD.

The AA provides the Super User/user with an interface to log onto and be authenticated for access to the HDD being protected by the SDV®. The user enters a username and pass-phrase combination that is used for authentication. The AA is used to:

- Authenticate a user access at pre-boot time, and then allows OS to boot
- Change the user passphrase, once authenticated

2.2 Cryptographic Boundary

The SDV® cryptographic boundary consists of the printed circuit board, components, FPGA logic, firmware, and interfaces. This logically encompasses:

- the Authentication Application (AA) which controls identification and authentication
- the NIOS Microprocessor which controls data flow between the host computer and the encryption/decryption engine
- the encryption/decryption engine which provides secure encrypted data storage of the host computer hard disk drive (HDD)

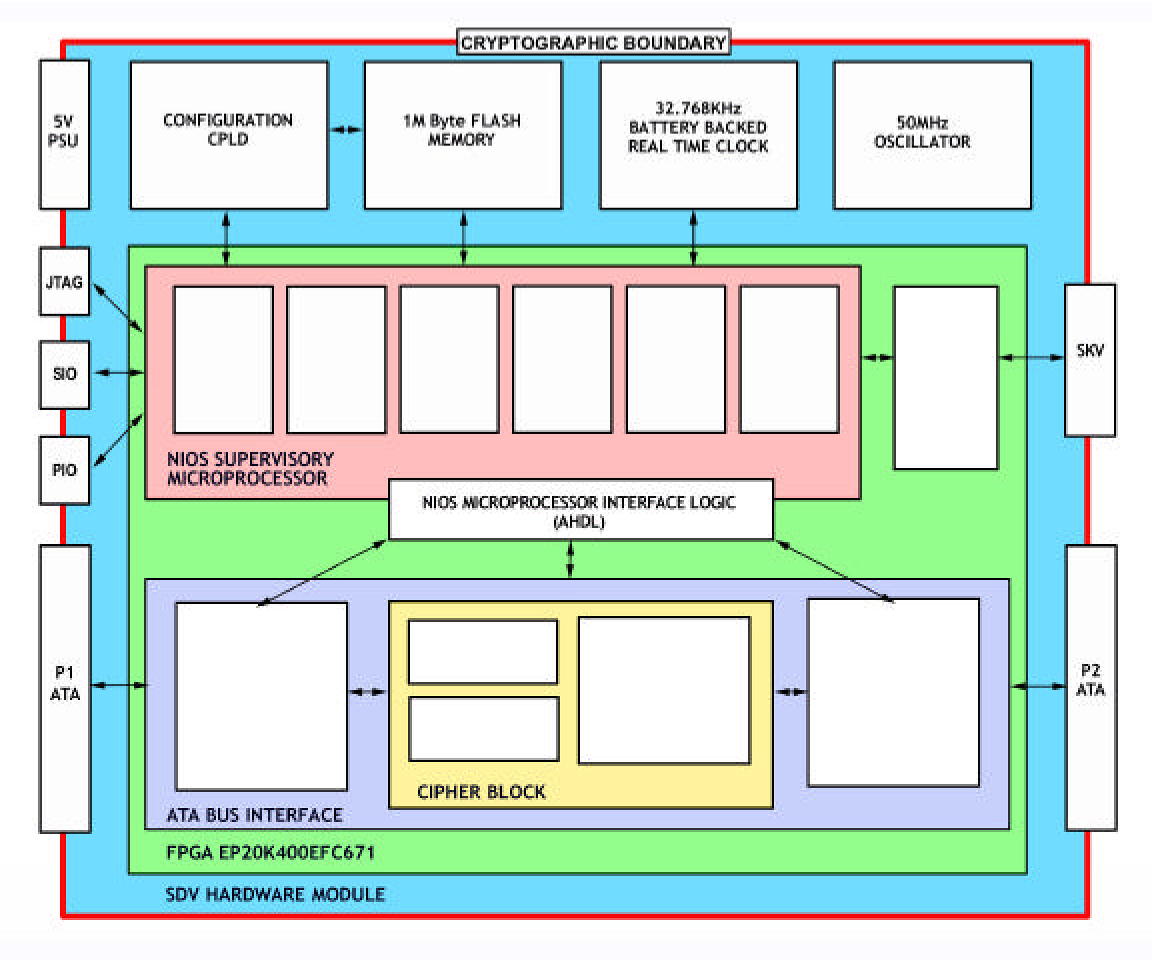

Figure 2. SDV® Cryptographic Boundary

2.3 SDV® Interfaces

The SDV® utilizes the following logical and physical interfaces:

Table 3. SDV® FIPS Interfaces

Interface	Description
Data Input Interface	The host data interface performs the data input function when data is being written to the HDD. The device data interface performs the data input function when data is being read from the HDD.
Data Output Interface	The host data interface performs the data output function when data is being read from the HDD. The device data interface performs the data output function when data is being written to the HDD.
Control Input Interface	The control input interface is a logical interface called the NIOS Microprocessor Interface. This interface controls the data flow through the cipher block during HDD read and write operations.
Status Output Interface	The host data interface is used to communicate with the AA which displays status output on the host computer's graphic interface, during authentication. The serial interface can also download status information.

Table 4. SDV® Physical Interfaces

Interface	Description
Host Data Interface P1 ATA	The host data interface transfers unencrypted data between the SDV® and the host PC mother board via an ATA 5 compliant interface. This interface is also used to transfer the Authentication Application software from the SDV® to the host BIOS during startup.
Device Data Interface P2 ATA	The device data interface transfers unencrypted data bi-directionally from the SDV® to the hard drive during the FIPS non-approved INSTALL mode and encrypted data bi-directionally during FIPS 140-2 Approved SECURE mode. The interface is ATA 5 compliant.
JTAG Interface	An IEEE standard 1149.1 Joint Test Action Group (JTAG) interface is provided for in-system programmability (ISP) and boundary scan testing (BST).
Proprietary Interface	The PIO interface consists of expansion connectors J1 and J2. This provides access to the JTAG interface and Serial Interface, as well as signals for general purpose system expansion.
Serial Interface	Pins on J2 are used as a serial interface which can be utilized to output status.
SKV (Serial) Interface (not enabled in FIPS Certified SDV®)	For the SDV201B - The SKV interface consists of connectors P4 and J3. This interface port provides a means by which the SDV® can communicate with an external authentication device. For the SDV18A - The SKV interface is provided as part of the PIO interface located at the J2 expansion port connector.
Power Interface (5V PSU)	The supply voltage required for the SDV201B is derived from the main 5V power supply of the host computer. A standard floppy disk drive power connector is used for connection of the +5V supply. The supply voltage required for the SDV18A is derived from the main 5V power supply of the host computer.

3. SDV® Access Control Policy

The SDV® controls access through strong role-based authentication using SHA-1, SHA-1 Cert. #219, and data encryption using AES 128-bit ECB, AES Cert. # 316.

3.1 Roles Supported

The SDV® cryptographic module supports two roles only: Super User and User. There is no Maintenance Role used with the SDV®.

3.1.1 Super User Role

This role is invoked when a user profile is set to Super User and the Super User Username and Passphrase are authenticated.

This role is given read/write access to all partitions after successful authentication any time the PC is powered on (booting from the HDD).

Only this role may use the administration services on the Systems Administrative Utility (SAU) CD, after successful Super User authentication.

3.1.2 User Role

This role is invoked after authentication when a user profile is set to User. This role remains active until the computer is powered off.

3.2 Authentication Required

SDV® Authentication is role-based. The SDV® requires a username and passphrase combination for both the Super User and user roles. See table below:

Table 5. SDV® Role/Authentication Policy

Role	Authentication Type	Authentication Strength	Type
Super User	Username	Min 4 - Max 54 Characters	Role Based
	Passphrase	Min 6 - Max 54 Characters	
User	Username	Min 4 – Max 54 Characters	Role Based
	Passphrase	Min 6 - Max 54 Characters	

The passphrase is case sensitive and can consist of any keyboard characters, including alpha, numeric, punctuation, and spaces (93 possible choices).

A minimum of six characters in the passphrase ensures less than one in one million probability of false acceptance.

The SDV ensures less than one in one hundred thousand per minute probability of false acceptance by requiring power down and restart after three failed authentication attempts.

3.3 Services Provided by the SDV®

There is no service provided by the SDV® for which the operator is not required to assume an authorized role; therefore no service is provided that would modify, disclose, or substitute cryptographic keys and CSPs, or otherwise affect the security of the SDV®. The following paragraphs describe each specific service of the SDV®.

3.3.1 SDV® Initialization

This administrative service, utilizing the SAU, consists of:

- **Synchronizing the RTC.** The SDV® synchronizes the SDV® Real Time Clock (RTC) to the computer RTC.
- **Configuring the Stealth Partition.** The SDV® selects the last partition configured to be the stealth partition, used exclusively by the SDV® for logging and administrative purposes.
- **Creating the Super User Account.** The Super User enters a username/ passphrase combination and other configuration parameters to set up the account that allows SDV® configuration and administrative services to be utilized.

3.3.2 Backup of Selected Partitions to Stealth Partition

This administrative service, utilizing the SAU, allows pre-selected partitions to be periodically backed up by the Super User, using the SAU.

3.3.3 Recovery/Restore Functions

This administrative service, utilizing the SAU, allows the Super User to:

- **Recover Backup Partitions:** restores previously backed up partitions.
- **Force the SDV® into INSTALL mode:** zeroizes all keys, restores the SDV® to INSTALL mode, and destroys the HDD configuration.
- **Restore the HDD to Unencrypted Format (non FIPS 140-2 Approved mode):** decrypts selected partitions, zeroizes all keys and restores the SDV® to INSTALL mode.

3.3.4 Creation of User Profile(s)

This administrative service allows the Super User, utilizing the System Administrative Utility (SAU), to create a User Profile defining the partition access rights for each user. Access rights are confined to *Read-only*, *Read/Write* or *No Access*.

3.3.5 Event Log Viewing

The SDV® documents user activity, specifically successful logons and unsuccessful logon attempts, in the events log. This administrative service, utilizing the SAU, allows the Super User to view the events log.

3.3.6 Updating the SDV® RTC (to the computer RTC)

This administrative service, utilizing the SAU, allows the Super User to update the SDV® RTC to the CMOS RTC.

3.3.7 Authenticate User/Super User

This service uses the AA to authenticate the User/Super User and enable FIPS 140-2 Approved secure operations.

3.3.8 Encryption of Data

This service uses the partition key to encrypt all data written to the HDD using the FIPS 197 Approved AES 128 ECB algorithm on a sector-by-sector basis. Each disk sector is a fixed length made up of 32 AES cipher blocks. The second layer of the implemented protocol involves scrambling each sector of data using a 128 bit linear feedback shift register and IGE block chaining of the 32 AES cipher blocks.

3.3.9 Decryption of Data

This service uses the partition key to decrypt all data read from the HDD using the FIPS 197 Approved AES 128 ECB algorithm on a sector-by-sector basis.

3.3.10 Hashing

This service is used in the FIPS Approved RNG to create secret keys and hash the passphrase for authentication.

3.3.11 Zeroization

This service deletes all keys when the Super User initiates the ‘Forced to Install Mode’ service, and ‘Restore the HDD to Unencrypted Format (non FIPS 140-2 Approved mode)’.

3.3.12 Show Status

The SDV® provides the Super User and User of the module with a “show status” service that allows the operator the ability to determine the state of and receive status information from the module.

3.3.13 Power-On Self Tests

The SDV® performs the following self tests and peripheral initialization procedures before it updates its status as “ready” and starts waiting for host commands.

- **Firmware integrity test:** FIPS 140-2 requires firmware to perform software integrity test. The CRC-32 checksum is calculated and compared with pre-computed value.

- **Known value test for AES and SHA-1**: Known value tests for both cipher and hashing algorithms (AES and SHA-1) are performed to satisfy FIPS 140-2 requirement.

3.3.14 Conditional Tests

- **Continuous RNG Test:** The first 64 bits generated after power-up, initialization, or reset are not used, but are saved for comparison with the next 64 generated bits. Each subsequent generation of 64 bits are compared with the previously generated 64 bits. The test fails if any two compared bit sequences are equal.

3.4 Services Allocated to Roles

The following table depicts the SDV® Services with the mode of operation and the role(s) allowed to use these services.

Table 6. SDV® Services Allocated to Roles

Service	General Mode of Operation	Role(s) Using Service
SDV® Initialization: , Stealth Partition Configuration, Super User Account Creation	INSTALL (Administrative)	Super User
Backup of Selected Partitions	INSTALL (Administrative)	Super User
Recovery of Backed up Partitions	INSTALL (Administrative)	Super User
Creation of User Profile(s)	INSTALL (Administrative)	Super User
Event Log Backup and Viewing	INSTALL (Administrative)	Super User
Update SDV® Real Time Clock	INSTALL (Administrative)	Super User
Authentication of Super User/User	SECURE (FIPS 140-2 Approved)	User/Super User

Encryption of Data	SECURE (FIPS 140-2 Approved)	User/Super User
Decryption of Data	SECURE (FIPS 140-2 Approved)	User/Super User
Hashing	SECURE (FIPS 140-2 Approved)	User/Super User
Zeroization	SECURE (FIPS 140-2 Approved)	Super User
Show Status	INSTALL (Administrative) SECURE (FIPS 140-2 Approved)	User/Super User
Power-On Self Tests	SECURE (FIPS 140-2 Approved)	User/Super User
Conditional Tests	SECURE (FIPS 140-2 Approved)	User/Super User

3.5 Access Rights within Services

The module includes the following Secret Keys and CSPs: Partition Key, Configuration Key, Passphrase Key, and the User Profile and Access Table. The following table lists the accessible cryptographic keys, critical security parameters (CSP) used and the type of access allowed for each service offered by the SDV®.

Table 7. SDV® Access Right within Services

Service	Cryptographic Keys and CSPs	Type of Access
SDV® Initialization	User Profile and Access Table	Read/Write
Backup of Selected Partitions	Partition Key	Read/Execute
Recovery of Backed up Partitions	Partition Key	Read/Execute
Create User Profile	Passphrase User Profile and Access Table	Write Write
Event Log Backup and Viewing	None	N/A
Authentication of Super User/User	Passphrase User Profile and Access Table	Read/Write Read Only
Control of Disk Access	User Profile and Access Table	Read Only
Encryption of Data	Partition Key Configuration Key	Read/Execute Read/Execute
Decryption of Data	Partition Key Configuration Key	Read/Execute Read/Execute
Hashing	None	N/A
Zeroization	All keys	Delete
Show Status	None	N/A
Power On Self Tests	None	N/A
Conditional Tests	None	N/A

4. SDV® Operation

The SDV® has two modes of operation: **INSTALL** and **SECURE** (FIPS 140-2 approved mode).

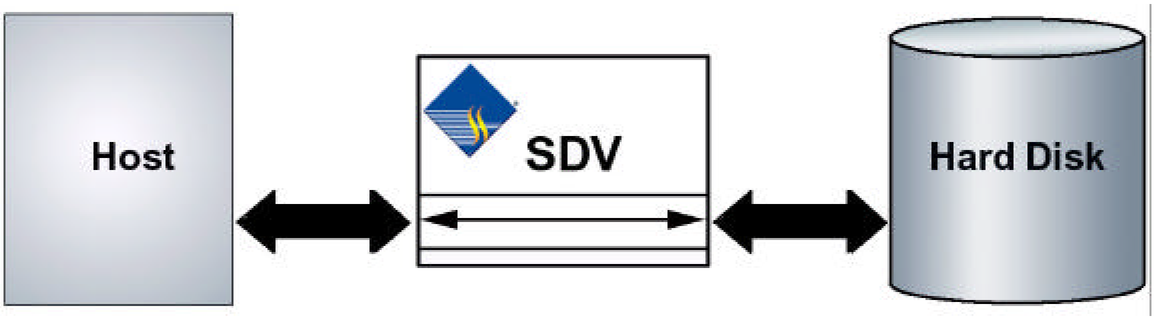

Figure 3. SDV® INSTALL Mode Illustrated

Initially the SDV® operates in **INSTALL** mode, which allows the Super User to create partitions, install an operating system (OS) and additional software as desired.

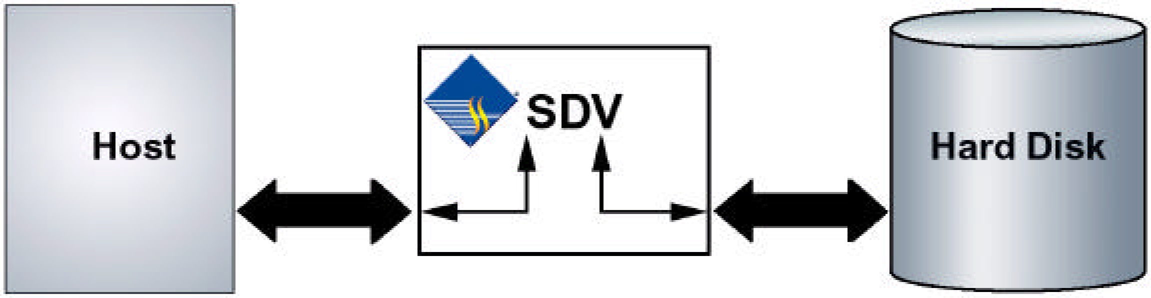

Figure 4. SDV® SECURE (FIPS 140-2-Approved) Mode Illustrated

When the Super User has installed the host computer's OS and is ready to configure the SDV®, the computer is booted from the System Administrative Utility (SAU) CD. Before entering the FIPS 140-2 Approved **SECURE** mode, the Super User must configure the SDV® while in **INSTALL** mode. At this point, the Super User may choose not to encrypt the HDD.

FIPS 140-2 Approved **SECURE** mode is enabled when the Super User elects encryption. In **SECURE** mode, the SDV protects the hard disk from any unauthorized access and gives the Super User the option to configure the SDV per requirements. The AES ECB (Cert. #136) cipher algorithm is used to encrypt/decrypt data. Further, the module uses the Infinite Garble Extension (IGE) block chaining to enable the encryption of an entire disk sector in 12-clock cycles.

5. Physical Security Policy

Both the SDV201B REV B and SDV18A REV A multichip embedded SDV® are installed and connected inside the casings of the computers they are protecting.

In a desktop PC, the SDV201B REV B is installed over a slot position normally used for the installation of expansion cards. After installation, the cover of the PC is replaced. The physical security of the SDV® relies on its location within the closed case of the computer.

In a laptop PC, the SDV18A REV A HDD Assembly replaces the existing HDD. After SDV® physical installation, the laptop cover is replaced. The physical security of the SDV® relies on its location within the closed case of the laptop.

It is required that the host computer undergo regular inspections to ensure tampering of the SDV® has not occurred.

6. Operating Environment

The SDV® does not have an underlying operating system. The SDV® operating environment is implemented in firmware controlled softcore FPGA and is non-modifiable.

7. Key and CSP Generation

The SDV® employs four keys and CSPs: The partition and configuration keys, and the Passphrase and the User Profile & Access Table CSPs. The SDV® protects keys and critical security parameters from disclosure, modification, or substitution. Keys/CSPs are stored in encrypted form on the stealth partition or in plaintext on the FLASH memory of the module. The Secret Keys are generated using the FIPS Approved RNG. All keys are zeroized by issuing of the zeroization service by the Super User.

8. FCC EMI/EMC Requirements

The SDV® hardware models, SDV18A REV A and SDV201B REV B, have been tested and found to comply with the limits for radiated and conducted emissions set by the following standards for a class "B" digital device.

- AS/NZS 3548:1995 (C15PR22) Class B
- FCC Part 15 Class B Unintentional Radiators ANSI C63.4 – 1992

9. Self Tests

Power-On Self Tests and Conditional Tests are described as services in Section 3, Paragraphs 3.3.12 and 3.3.13, respectively. The SDV® performs the following self-tests:

Table 8. SDV® Self-Tests

Test	Description
Software/Firmware Integrity Test	The SDV® calculates a CRC-32 checksum which is compared with a pre-computed value.
AES Algorithm Test	The AES algorithm is tested for encrypt and decrypt using a Known Answer Test in the Electronic Code Book (ECB) mode of operation.
SHA-1 Algorithm Test	The SHA-1 hash algorithm is tested using a Known Answer Test.
RNG Conditional Test	The SDV® seeds the pseudo RNG at startup and saves the first output value to compare with subsequent RNG values. A new value is generated if a generated value is the same as he previously stored value.

All data output via the SDV® Data Interfaces is disabled during Power-up Self Tests or when an error state exists. The SDV® enters an error state upon failure of any of the self-test routines. The module does not perform any cryptographic functions while in an error state. An error state is exited by powering the SDV®-protected computer off and then back on.

10. Mitigation of Other Attacks Policy

10.1 Dictionary Attack

To protect data against dictionary attacks, SHA1 is used on the host PC's processor for the iterated hash of the passphrase because it is the fastest software hash, compared to using an AES based hash that involves re-keying, such as a Davies-Meyer hash. It is necessary to make the iterated hash as fast as possible in software so that the attacker who uses special hardware to do dictionary attacks will be slowed down.

11. Glossary

The following are abbreviations, acronyms, and terms in this document:

Table 9. SDV® Security Policy Glossary

Acronym/Term	Definition
AA	The Authentication Application is an embedded software/firmware application that provides the user interface for the SDV®-protected PC during normal operations. The AA is stored within and loaded from the SDV® when the system is selected as the PC boot media.
AES	The Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies and, as a likely consequence, may eventually become the de facto encryption standard for commercial transactions in the private sector. (Encryption for the US military and other classified communications is handled by separate, secret algorithms.)
Algorithm	A procedure or formula for solving a problem. The word derives from the name of the mathematician, Mohammed ibn-Musa al-Khwarizmi (780 – 850), a member of the royal court in Baghdad.
ATA	Advanced Technology Attachment is the official name that American National Standards Institute group X3T10 uses for what the computer industry calls Integrated Drive Electronics (IDE).
Authentication	A process of determining someone or something is who or what it is declared to be, commonly accomplished through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic.
BIOS	Basic Input/Output System, the program a personal computer's microprocessor uses to start the system when power is switched on, also manages data flow between the computer's operating system and attached devices such as the hard drive, video adapter, keyboard, mouse, and printer.
Block	A block is a contiguous set of bits or bytes that forms an identifiable unit of data.
Boot	To boot (as a verb; also "to boot up") a computer is to load an operating system (OS) into the computer's main memory or random access memory (RAM). Once the OS is loaded, it's ready for users to run applications.
Chip	"Chip" is short for microchip (also called IC or integrated circuit), the complex yet tiny modules that store computer memory or provide logic circuitry for microprocessors. Manufactured from a silicon (or, in some special cases, sapphire) wafer, a chip is first cut to size and then etched with circuits and electronic devices.
Cipher	Sometimes used as a synonym for ciphertext, but it more usually means the method of encryption rather than the result.
Ciphertext	Encrypted text; the result of encrypting plaintext.
CMOS	Complementary Metal Oxide Semiconductor, the semiconductor technology used in the transistors manufactured into most of today's microchips. CMOS transistors use almost no power when not needed.
Configuration	The arrangement or process of arranging the parts that make up a whole. In computers, a configuration often refers to the specific hardware and software details in terms of devices attached, capacity or capability, and exactly what the system is made up of.
CPU	Central Processing Unit (CPU) is an older term for processor and microprocessor, the central unit in a computer containing the logic circuitry that performs the instructions of a computer's programs.
CSP	Critical Security Parameter
Decryption	The process of converting encrypted data back into its original form, so it can be understood.
DMA	Direct Memory Access (DMA) is a capability provided by some computer bus architectures that allows data to be sent directly from an attached device (such as a disk drive) to the memory on the computer's motherboard. The microprocessor is freed from involvement with the data transfer, thus speeding up overall computer operation.
Encryption	The conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people.
ESD	Electrostatic Discharge (ESD) is the release of static electricity when two objects come into contact. Familiar examples of ESD include the shock we receive when we walk across a carpet and touch a metal doorknob and the static electricity we feel after drying clothes in a clothes dryer.
FAT	A File Allocation Table (FAT)is a table maintained by an OS on a HDD. It provides a map of the clusters (the basic units of logical storage on a hard disk) that a file has been stored in.
FPGA	A Field-Programmable Gate Array (FPGA) is an integrated circuit (IC) that can be programmed in after manufacture. FPGAs are used by engineers in the design of specialized ICs that can later be produced hard-wired in large quantities for distribution to computer manufacturers and end users. Ultimately, FPGAs might allow computer users to tailor microprocessors to meet their own individual needs.

Acronym/Term	Definition
GUI	A GUI (usually pronounced GOO-ee) is a Graphical User Interface to a computer. When you read from the internet, you are looking at the GUI or graphical user interface of your particular Web browser.
Hash	Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string.
HDD	A Hard Disk Drive, in a personal computer, is the mechanism that controls the positioning, reading, and writing of the hard disk, which furnishes the largest amount of data storage for the PC. Although the hard disk drive (often shortened to "hard drive") and the hard disk are not the same thing, they are packaged as a unit and so either term is sometimes used to refer to the whole unit.
IBM	International Business Machines
IDE	Integrated Drive Electronics (IDE) is a standard electronic interface used between a computer motherboard’s data paths or bus and the computer's disk storage devices. The IDE interface is based on the IBM PC Industry Standard Architecture (ISA) 16-bit bus standard, but it is also used in computers that use other bus standards .
IGE	Infinite Garble Extension – a type of Cipher Block Chaining (See CBC)
Initialization	The process of locating and using the defined values for variable data used by a computer program. For example, an operating system is installed with default or user specified values that determine certain aspects of how the system or program is to function. Typically, these values are stored in initialization files.
Key	In cryptography, a key is a variable value is applied using an algorithm to a string or block of unencrypted text to produce encrypted text, or to decrypt encrypted text. The length of the key is a factor in considering how difficult it will be to decrypt the text in a given message.
LBA	Logical Block Addressing (LBA) is a technique that allows a computer to address a hard disk larger than 528 megabytes. A logical block address is a 28-bit value that maps to a specific cylinder-head-sector address on the disk. Logical block addressing is one of the defining features of Enhanced IDE (EIDE), a hard disk interface to the computer bus or data paths.
Logon	The procedure used to gain access to an operating system or application, usually in a remote computer. Almost always a logon requires that the user have (1) a user ID and (2) a password.
MB	As a measure of computer processor storage and real and virtual memory, a megabyte (abbreviated MB) is 2 to the 20th power bytes, or 1,048,576 bytes in decimal notation.
MBR	The Master Boot Record (MBR) is the information in the first sector of any hard disk or diskette that identifies how and where an OS is located so that it can be boot (loaded) into the computer's main storage or random access memory (RAM).
NTFS	NT or sometimes New Technology File System
‘on the fly’	In relation to computer technology, "on the fly" describes activities that develop or occur dynamically rather than as the result of something that is statically predefined.
OS	An operating system is the program that, after being initially loaded into the computer by a boot program, manages all the other programs in a computer.
Passphrase	A string of characters longer than the usual password, used in creating a digital signature. For example, the SDV® II requires a passphrase of between 6 and 54 characters when you authenticate.
Password	A password is an unspaced sequence of typically between four and 16 characters used to determine a computer user requesting access to a computer system is really that particular user.
PC	Personal Computer
PIO	Programmed Input/Output (PIO) is a way of moving data between devices in a computer in which all data must pass through the processor. A newer alternative to PIO is Direct Memory Access (DMA)).
Plaintext	Text before it has been encrypted.
PRNG	A Pseudo-Random Number Generator (PRNG) is a program written for, and used when large quantities of random digits are needed. Most of these programs produce endless strings of single-digit numbers, usually in base 10. When large samples of pseudo-random numbers are taken, each of the 10 digits in the set {0,1,2,3,4,5,6,7,8,9} occurs with equal frequency, even though they are not evenly distributed in the sequence.
RAM	Random Access Memory (RAM) is the place in a computer where the OS, application programs, and data in current use are kept so that they can be quickly reached by the computer's processor. The data in RAM stays there only as long as the computer is running.
Random Numbers	Random numbers are numbers that occur in a sequence such that two conditions are met: (1) the values are uniformly distributed over a defined interval or set, and (2) it is impossible to predict future values based on past or present ones.
RTC	A Real-time Clock (RTC) is a battery-powered clock included in a microchip in a computer motherboard. This chip is usually separate from the microprocessor and other chips and is often referred to simply as the CMOS. A small memory on this chip stores system description or setup values, including current time values (for the year, month, date, hours, minutes, and seconds) stored by the RTC. When the computer is turned on, the BIOS stored in the computer's ROM microchip reads the current time from the memory in the chip with the real-time clock.

Acronym/Term	Definition
Salt	In password protection, salt is a random string of data used to modify a password hash. Salt can be added to the hash to prevent a collision by uniquely identifying a user's password, even if another user in the system has selected the same password. Salt can also be added to make it more difficult for an attacker to break into a system by using password hash-matching strategies because adding salt to a password hash prevents an attacker from testing known dictionary words across the entire system.
SAU	The System Administrative Utility is a software application, stored on a CD, which allows the super user (crypto-officer, system administrator) to perform a variety of functions to administer the SDV®-protected system. The SAU is the first application the super user will need to run to initialize and configure a newly installed SDV®.
SDV®	The Silicon Data Vault® is a Cryptographic Module (CM), installed into a PC, connected in-line between the host motherboard IDE controller and hard disk drive (HDD). It prohibits unauthorized computer access through strong user authentication while encryption and a sophisticated key management scheme enforce data protection.
SHA-1	Secure Hash Algorithm-1
SSL	Secure Systems Limited – the Australian-based research and development company that developed the Silicon Data Vault®.
Super User	Crypto Officer or System Administrator
Zeroization	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.