Secure Systems Limited

SDV® High Assurance (SDV®-HA) Series
Technical Overview

Glossary

The following glossary defines terms used in this document that are specifically established by Secure Systems. This glossary also includes definitions of terms used by Secure Systems that may differ from the definitions typically used in industry. Standard industry or third-party terms are not defined in this glossary.

Acronym/Term	Definition
AAU	The Authentication and Administration Utility (AAU) is a software application developed by Secure Systems to perform product functions such as initialisation, authentication and administration.
Anti-Tamper	Engineering activities intended to deter and/or delay exploitation of critical technologies in a system.
Data At Rest	Data stored in a disk or another medium that is not being actively used in processing or data transmission.
Fireguard	Fireguard is a hardened web browser application developed by Secure Systems which is based on the Firefox web browser.
Initialisation	The process of establishing security parameters to enable secure operation of a Secure Systems product.
MEE	A Mobile Execution Environment (MEE) is a hardened OS developed by Secure Systems which is based on the Ubuntu Linux OS.
PAA	The Portable Authentication Application (PAA) is a software application developed by Secure Systems that allows authentication to Secure Systems security products from Windows.
SDV	The Silicon Data Vault (SDV) is a Cryptographic Module (CM), incorporating an integral mass storage device. It prohibits unauthorised computer access through strong key management and user authentication while encryption enforces data protection.
SysAdmin	The System Administrator (SysAdmin) is a user role for managing the installation and configuration of a Secure Systems product.
SysUser	The System User (SysUser) is a user role for accessing the user data stored on a Secure Systems product.
Token	A token is a physical device containing a key that an authorised user is given to aid in authentication.

Document Revision History **File Name:** Technical Overview.odt **Title:** SDV-HA Series Technical Overview.			**Document Number:** SSL-ML-0032
Date: 21/12/2015	**Author:** T Adams	**Version:** 1.6	**Description:** Updated technical specifications.

Secure Systems Limited
Tel: +61 (8) 9240 8708
PO Box 602, Balcatta, Western Australia 6914
Email: secure@securesystems.com.au
ABN: 11 092 978 197
Web: www.securesystems.com.au

THE SILICON DATA VAULT HIGH ASSURANCE (SDV-HA)

SDV-HA OVERVIEW

The SDV-HA series is a High Grade device developed to meet Australian Government requirements for high assurance products securing TOP SECRET data while allowing the device to be stored and handled as UNCLASSIFIED with a dissemination limiting marker of For Official Use Only, when powered down or unauthenticated. The device will also allow SECRET data to be handled as UNCLASSIFIED, when powered down or unauthenticated.

The SDV-HA is a secure storage device that operates independently of the host PC's resources and is illustrated in Figure 1. The SDV-HA offers maximum protection of data-at-rest. Once the user has successfully authenticated, the SDV-HA operates like a standard external storage device, except all data is encrypted as it is written, and is decrypted as it is read from the device. Encryption ensures that secured data is inaccessible when the SDV-HA is not authenticated. No changes to system operation will be apparent whilst encryption is operating. As the SDV-HA cryptographic parameters are established during the Initialisation of the SDV-HA, no data can be written to the device prior to this process being performed by the administrator of the device.

The following product capabilities are provided in the SDV-HA:

1) Hardware based security that operates independently of the host PC's resources and is transparent to the host PC user after authentication.
2) Proven NSA Suite B cryptographic primitives used for fully encrypted, large capacity, solid state data storage.
3) Strong key management methodology, incorporating multiple factor user authentication, used to provide secure pre-boot and post-boot user authentication prior to gaining access to data storage.

Figure 1: SDV High Assurance

4) Independent User and Administrator roles with enforced access controls.
5) Effective system integrity checking methodologies, strong tamper protection methodologies and a secure decommissioning process.
6) USB and eSATA connection to host PC systems.
7) Support for pre-boot and post-boot authentication mechanisms.
8) Optional hardened OS (MEE) and software application (Fireguard) to be uploaded to a host PC to perform remote data processing, secure transactions or remote server access.

The SDV-HA provides strong anti-tamper mechanisms to minimise the risk of mechanical and electronic attempts to subvert the operation of the SDV-HA. In the case of a tamper event being detected, the SDV-HA clears critical security parameters thereby ensuring the data stored on the SDV-HA is protected against disclosure. If a tamper event occurs, the SDV-HA must be returned to an Authorised Maintenance Centre for data to be restored.

USER ROLES

The SDV-HA supports two user roles: the System Administrator (SysAdmin) who defines the SDV-HA configuration and administers the SDV-HA, and System User (SysUser) who accesses data on the SDV-HA following authentication. These two roles don't necessarily correlate to physical people depending on the usage of the SDV-HA within an organisation. For example, both the SysUser and SysAdmin roles could be performed by the same person for a particular SDV-HA.

AUTHENTICATION OVERVIEW

SDV-HA authentication is performed using a password and an authentication token. Authentication tokens are created for the SysAdmin and the SysUser using USB Flash Drives supplied with the SDV-HA, when the SDV-HA is initialised for use. Subsequently, the correct authentication token must be presented each time the SysAdmin or SysUser authenticates and must be removed from the device following authentication. The key stored on the token is updated each time authentication is performed and therefore a token that is copied is only valid for the subsequent authentication process. In the event that it is suspected that a token may have been copied then the SysAdmin or SysUser only needs to authenticate to invalidate the copied key.

The SDV-HA supports two modes of authentication that are known as pre-boot (authentication at host PC startup) and post-boot (authentication from within Windows); both authentication modes are available when the SDV-HA is connected to the host PC via the eSATAp port or via the USB port.

Pre-boot authentication occurs when the SDV-HA is connected to either the host PC's eSATAp or USB port and the SDV-HA is set as the first boot device. When the host PC is powered on, the SDV-HA interrupts the standard PC boot process to load the AAU to perform two factor authentication. Upon successful authentication the user can choose to boot either an OS installed on the SDV-HA or the OS installed on the host PC's internal disk drive. Once the OS is executed the user has access to the SDV-HA's data partitions.

Post-boot authentication occurs when the SDV-HA is connected to either the host PC's eSATAp or USB port whilst the host PC is already executing Windows. Upon connection, Windows detects the SDV-HA and the PAA is uploaded automatically or run manually by the user. Once executed, the PAA allows two factor authentication to be performed. User access to the SDV-HA's data partitions is possible upon successful authentication.

PHYSICAL INTERFACES

The SDV-HA has three (3) connector interfaces:

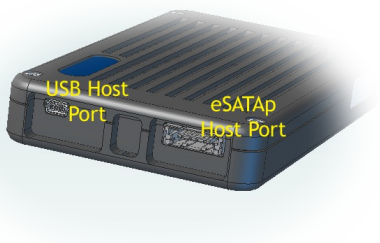

Figure 2: Host PC Interfaces

1) USB host port – A Mini-USB connector used to connect the SDV-HA to a host PC USB Type A connector with the supplied USB cable. See Figure 2. The SDV-HA is powered from the host PC USB port.
2) eSATAp host port – An eSATA connector to connect the SDV-HA to a host eSATAp connector with the cable supplied. See Figure 2. The SDV-HA is powered from the host PC eSATAp port.

   Note - In general, SDV-HA data performance is better when the eSATA connection is used rather than USB, as the USB connection is limited

to USB2 performance. However, a number of PCs don't support an eSATA connection, so in this case it is possible to use a USB3 to eSATA adapter, such as the Addonics ADU3ESA, for maximum performance.

3) Token port – The USB Type A connector is provided to allow connection of authentication tokens (i.e. a USB Flash Drive) during initialisation and authentication. See Figure 3.

Note - Only one host interface port can be used at a time (USB or eSATAp), otherwise damage may occur to the device.

A Status Indicator LED is provided next to the Token port as shown in Figure 3. Status indications are:

Off – No power is applied. Data-at-rest is secure.

Green – SDV-HA is unauthenticated. Data-at-rest is secure.

Orange – SDV-HA is authenticated. Data is accessible and is only as secure as the operating environment in use.

Red (flashing) – SDV-HA has responded to a tamper event or experienced an error and is in the fail-safe state. The data is protected and the SDV-HA is inoperable whilst in this state.

Figure 3: Token Interface

CONFIGURATION OPTIONS & STORAGE USE

The SDV-HA provides a high level of operational versatility through both its dual modes of connectivity and dual modes of authentication. The operational versatility of the SDV-HA allows it to be configured for numerous operational scenarios, including:

1. Bootable storage device with an installed OS for a specific PC, using pre-boot authentication.

   Note - The use of the SDV-HA's USB port in this scenario may be limited by the capabilities of the OS.

2. Portable storage device with an installed OS that can be booted from different PCs, using pre-boot authentication.
3. Data storage device accessed via a PC running Windows, using post-boot authentication.
4. Data transportation device where the SDV-HA is used to store data that can be accessed from different PCs running Windows, using post-boot authentication.

Irrespective of how the SDV-HA is configured access to data following successful pre-boot or post-boot authentication is always possible from a PC running Windows. Figure 4 is a conceptual model of the configuration options available using the SDV-HA.

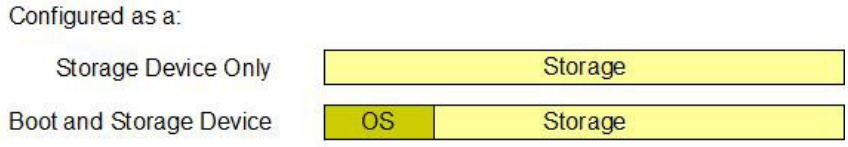

Figure 4: Conceptual Model of Configuration Options

Note - The use of the System and Guarded capabilities, as defined in the SDV High Assurance Series Manual - System and Guarded Capabilities Addendum document [SSL-ML-0039], provides additional configuration flexibility to that described above.

It is expected that the primary use of the SDV-HA will be as a storage device that is accessed in two alternative ways; from a PC running Windows (Operation From Windows) and as the first boot device for a PC (Operating as a Boot Device) where an OS, most likely Windows is booted from the SDV-HA.

During Initialisation the SDV-HA allows the creation of up to four data partitions to break up the provided storage area as required. This Initialisation partitioning function is provided to enable the product administrator to simply and rapidly configure the device for immediate use. Alternatively for more advanced configurations the Initialisation partitioning function can be skipped and the SDV-HA can be partitioned using a standard disk partitioning tool.

Note – Any data partitions created during Initialisation are automatically formatted as FAT32 to provide maximum compatibility with different operating systems. However, performance improvements (particularly write performance) are likely by re-formatting the partitions to a native partition format for the operating system on which the SDV-HA will be used (e.g. NTFS for Windows).

TECHNICAL SPECIFICATIONS SDV-HA (HIGH ASSURANCE)

Product Identification

Product Name:	SDV-HA (High Assurance)
Model Number:	SDV-HAxxx
Manufacturer:	Secure Systems Limited
Description:	Silicon Data Vault (SDV) secure high assurance portable execution and data storage device.

Electrical Specifications

Input Supply Voltage:	5VDC +/-5%
Input Supply Current: (240Gbyte Storage)	~250mA (startup) ~380mA (idle) ~500mA (accessing data) ~750mA (during Factory Reset)
Input Supply Current: (480Gbyte Storage)	~760mA (startup) ~400mA (idle) ~580mA (accessing data) ~940mA (during Factory Reset)
Power Supply Source:	USB/eSATAp Host Interface
Mean Time Between Failure (MTBF):	1 500 000 hours (**excluding battery replacement every 3 years)

Mechanical

Enclosure Construction:	Aluminium Alloy
Primary Protective Coating:	MIL-DTL-5541 Class 3 Conductive Alodine
Secondary Protective Coating:	Non-conductive Polymer Powder Coating
Length (Excluding Sleeve):	143 mm
Width (Excluding Sleeve):	81mm
Height (Excluding Sleeve):	20mm
Weight (Including ISD):	420 grams

External Interfaces

Host PC SATA Interface:	Combination eSATAp (1.5Gbps)
Host PC USB Interface:	Mini Type-B USB 2.0 (High Speed)
Token USB Interface:	Type-A USB 2.0 (Full Speed)
Status Indication:	Single Tri-colour status LED

Storage Specifications

Integral Storage Device (ISD):	1.8" ZIF PATA SSD ATA-5/6/7/8 Compatible
Secure Storage Capacity:	240 GBytes and 480 GBytes
Host USB Vendor ID (VID):	0x27B3
Host USB Product ID (PID):	0x0100

Security Specifications

Accreditation:	Australian Government High Assurance
Authentication:	Two Factor (Passphrase and Token)
Cryptography:	NSA Suite B Algorithms
Data Protection Level:	Up to and including Top Secret Classification

EMC/EMI Compliance

Radiated Emissions:	CISPR 22:2006 (C-Tick) Compliant
ESD Immunity:	Tested to ±8KV
Radiated Susceptibility:	Tested to 3V/m from 80MHz to 1 GHz
Transient Immunity:	Tested to ±2KV at 5KHz

Environmental Conditions

Temperature (Operational):	0ºC to +50ºC
Temperature (Storage):	-25ºC to +70ºC
High Temperature (Operational):	Tested to MIL-STD-810G Method 501.5 Procedure II (Level A2)
Low Temperature (Storage):	Tested to MIL-STD-810G Method 502.5 Procedure I (Level -25ºC)
Low Temperature (Operational):	Tested to MIL-STD-810G Method 502.5 Procedure II (Level 0ºC)
Temperature Gradient (Max):	4ºC per Minute
Humidity Range (Operational):	10% to 90% R.H. (No Condensation)
Humidity Range (Storage):	5% to 90% R.H. (No Condensation)
Altitude Range (Operational):	8,000ft (Pressurisation Above Sea Level)
Classical Shock Test:	Tested to IEC-60068-2-27 HS Peak of 15G for 11mS
Transport Vibration (Road):	Tested to MIL-STD-810G Method 514.6 Category 4
Transport Vibration (Aircraft):	Tested to MIL-STD-810G Method 514.6 Category 7
Transport Vibration (Rail):	Tested to MIL-STD-810G Method 514.6 Category 11
Operation Vibration (SEA):	Tested to MIL-STD-167-1A Type I – Environmental Vibration
Transit Drop Test:	Tested to MIL-STD-810G Method 516.6 Procedure IV
PCB Conformal Coating:	MIL-1-46058C / IPC-CC-830 Approval
Flammability Rating:	Low

