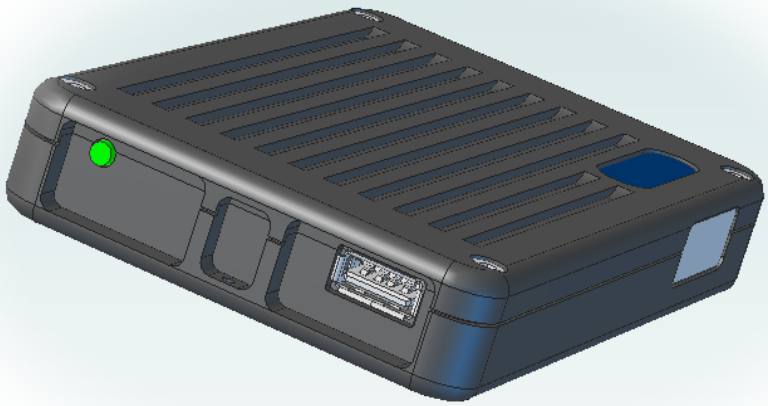
Secure Systems Limited

SDV® High Assurance (SDV®-HA) Series (Rev 1 & Rev 2) 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.
Initialisation	The process of establishing security parameters to enable secure operation of a Secure Systems product.
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 Technology	The Silicon Data Vault (SDV) technology refers to the sophisticated security functionality developed by Secure Systems and implemented in hardware and software. The technology encompasses: strong key management; multi-factor authentication; full disk encryption; code signing; and tamper detection and response. The SDV technology has been incorporated into a range of SDV secure data at rest products.
SDV3	The SDV3 is the third generation of the Silicon Data Vault (SDV) technology.
SDV-HA	The SDV-HA is an ASD certified High Assurance/Grade external storage product developed as an extension of the SDV3.
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: 27/10/2023	**Author:** T Adams	**Version:** 1.11	**Description:** Minor specifications update.

Secure Systems Limited
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 Assurance external storage device for protecting data-at-rest. The SDV-HA has been developed to meet Australian Government requirements for high assurance products securing data up to and including TOP SECRET, while allowing the device to be stored and handled as PROTECTED when powered down or unauthenticated. The SDV-HA will also similarly allow SECRET (or lower classification) data to be handled as PROTECTED, when powered down or unauthenticated. Note, SDV-HA devices are available in two different hardware revisions (Rev 1 & Rev 2), both of which are covered by this document and specifically referred to where required.

The SDV-HA is a pocket-sized portable storage device that offers maximum protection of data-at-rest by providing key features such as CNSA Suite (formerly NSA Suite B) encryption, active tamper protection and two factor authentication. The SDV-HA is illustrated in Figure 1. The SDV-HA is ideal for various remote and office-based environments that require strong data-at-rest protection, ensuring that secured data is inaccessible when the SDV-HA is not authenticated. Once the user has successfully authenticated, the SDV-HA operates like a standard external storage device, with data encrypted and decrypted transparently to the user. The following key product capabilities are provided by the SDV-HA:

1) Hardware based security, built with a secure design architecture that operates independently of the host PC's resources (i.e. the SDV-HA is fully self contained) and is transparent to the host PC user after authentication.
2) Proven CNSA Suite (formerly NSA Suite B) cryptographic algorithms used for fully encrypted, large capacity (240GB, 480GB or 960GB), solid state data storage.

Figure 1: SDV High Assurance

3) Strong key management methodology, incorporating multiple factor user authentication, used to provide secure user authentication prior to gaining access to data storage.
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 (type dependent on hardware revision) and eSATA (Rev 1) connections to host PC systems.
7) Support for pre-boot and post-boot authentication mechanisms. Pre-boot authentication utilises the AAU authentication application, while post-boot authentication utilises the PAA authentication application. Both authentication applications are loaded from the SDV-HA itself.
8) Support for booting and operating an OS directly from the SDV-HA storage, allowing a PC to be operated without any internal storage.
9) Support for seperately storing and independently accessing data at two different classification levels, i.e. a dual classification capability. **Note, the storage of lowly classified data on the SDV-HA is not yet certified for use, so is currently disabled.**

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 (when the SDV-HA is initialised for use), using the USB tokens supplied with the SDV-HA. 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 authentication information stored on the token is updated each time authentication is performed.

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 supported for all host PC interfaces provided by the SDV-HA (based on the hardware revision).

Pre-boot authentication occurs when the SDV-HA is connected to the host PC 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 (either UEFI or legacy BIOS) to load the AAU to perform two factor authentication for either the SysUser or SysAdmin. 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 storage. 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 the host PC whilst the host PC is already executing Windows. Upon connection, Windows detects the SDV-HA and the PAA is uploaded automatically or can be run manually by the user. Once executed, the PAA allows two factor authentication to be performed for the SysUser (post-boot authentication for the SysAdmin is not supported). User access to the SDV-HA's data partitions is available upon successful authentication.

AUTHENTICATION USAGE

The two modes of authentication supported by the SDV-HA for the SysUser provide flexibility to use each authentication method in different scenarios. Some example scenarios for when pre-boot authentication may be preferred are:

- When the SDV-HA contains the OS.
- When the SDV-HA is utilised with a host PC that does not have any additional storage devices (i.e. the SDV-HA is the only storage device and contains the OS).

Some example scenarios for when post-boot authentication may be preferred are:

- When the SDV-HA is used with a host PC that is typically ‘always on’.
- When the SDV-HA is being used as a data transfer device between multiple host PCs.

ANTI-TAMPER

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. The SDV-HA will also enter the fail-safe state at

the time of the tamper event or when the SDV-HA is next powered on. If a tamper event occurs, the SDV-HA must be returned to an Authorised Maintenance Centre (AMC) for data to be restored.

PHYSICAL INTERFACES

The SDV-HA has two different hardware revisions, referred to as Rev 1 and Rev 2. The physical interfaces provided by each hardware revision have some commonality, but also differences, as described in the following sections.

HOST PC INTERFACES (REV 2)

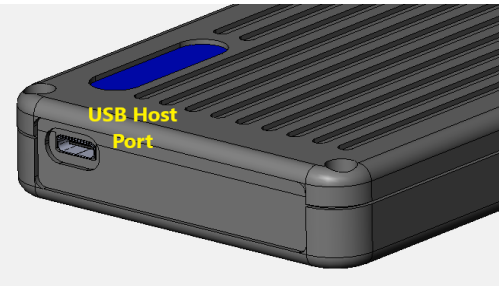


Figure 2: Host PC Interfaces (Rev 2)

The SDV-HA (Rev 2) has a single host PC interface; a USB Type-C connector used to connect the SDV-HA (Rev 2) to a host PC Type-C port with the supplied USB cable. See Figure 2. The SDV-HA (Rev 2) is powered from the host PC USB port when using this interface.

Note - It is strongly recommended that the SDV-HA (Rev 2) is ONLY used with a USB port that provides 3A (i.e. 15W) of power.

HOST PC INTERFACES (REV 1)

The SDV-HA (Rev 1) has two (2) host PC interfaces:

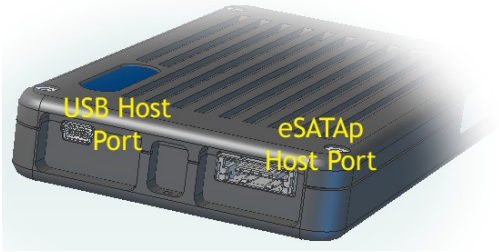


Figure 3: Host PC Interfaces (Rev 1)

1) USB host port – A Mini-USB connector used to connect the SDV-HA (Rev 1) to a host PC USB Type A port with the supplied USB cable. See Figure 3. The SDV-HA (Rev 1) is powered from the host PC USB port when using this interface.
2) eSATAp host port – An eSATA connector used to connect the SDV-HA (Rev 1) to a host eSATAp port with the supplied eSATAp cable. See Figure 3. The SDV-HA (Rev 1) is powered from the host PC eSATAp port when using this interface.

Note - In general, SDV-HA (Rev 1) data performance is better when the eSATA connection is used rather than USB, as the USB connection is limited to USB2 performance. However, an eSATA connection is not typically provided by modern PCs, so in this case it is possible to use a commercially available USB3 (or USB3.1) to eSATA adapter for maximum performance. Similarly, Thunderbolt to eSATA adapters can also be used in some cases. It is recommended to contact Secure Systems to discuss available options.

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

TOKEN INTERFACE AND LEDS

A USB Type A connector is provided to allow connection of authentication tokens (i.e. USB tokens) during initialisation and authentication. See Figure 4. The token port is provided on both SDV-HA hardware revisions.

A Status LED is provided as shown in Figure 4. The Status LED is provided on both SDV-HA hardware revisions.

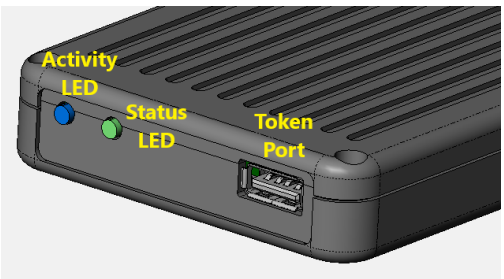


Figure 4: Token Interface

Status indications are:

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

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

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

Red (flashing) – The SDV-HA has experienced a significant error (including, but not limited to, detection of a tamper event) and is in the fail-safe state. The status LED can flash at two rates; fast (5 flashes per second) for a tamper event and slow for all other errors (2 flashes per second). The data is protected and the SDV-HA is inoperable whilst in this state. Depending on the error, the fail-safe state can be resolved by power cycling the SDV-HA or will remain indefinitely (requiring maintenance).

An Activity LED is provided as shown in Figure 4 for SDV-HA Rev 2 hardware only. The Activity LED indicates when data is being actively accessed on the SDV-HA (Rev 2) by the host PC; data activity is shown throughout operation. During data activity, the Activity LED will flash at a faster rate (10 flashes per second) for USB 3.X operation and a slower rate (5 flashes per second) for USB 2.0 operation. When the USB interface is in a suspend state, the activity LED will slowly fade off and on.

DUAL CLASSIFICATION

Note, the storage of lowly classified data on the SDV-HA is not yet certified for use, so is currently disabled.

The SDV-HA primarily supports the data at rest protection of highly classified data (e.g. TOP SECRET), but the SDV-HA also optionally supports storage and protection of lowly classified data (e.g. PROTECTED). Support for seperately storing and independently accessing both highly and lowly classified data is referred to as a dual classification capability. The storage of lowly classified data is optionally configured during SDV-HA Initialisation.

The primary storage area refers to the SDV-HA storage portion configured for highly classified data storage, whereas the secondary storage area similarly refers to the lowly classified data storage portion. When both storage areas are configured and the SysUser authenticates the same SysUser password is used, but each storage area utilises a different SysUser token. The SysUser tokens for authentication of each area are referred to as the primary and secondary SysUser tokens.

CONFIGURATION OPTIONS & STORAGE USE

The SDV-HA provides a high level of operational versatility through its dual modes of connectivity and ability to support storage of data at two different classification levels; allowing the SDV-HA to be configured for several 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.

When the SDV-HA is configured for dual data classification levels, then each of the above operational scenarios can be applied to each data classification level independently, offering even more operational versatility.

Figure 5 is a conceptual model of the configuration options available using the SDV-HA, where the SDV-HA has been configured for single classification access.

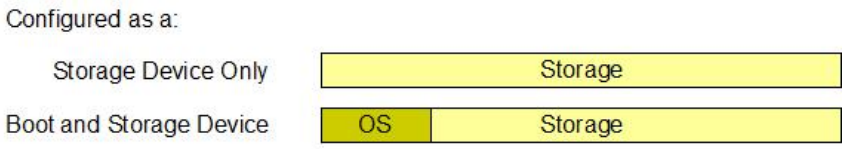


Figure 5: Conceptual Model (Single Classification)

Figure 6 is a conceptual model of the configuration options available using the SDV-HA, where the SDV-HA has been configured for dual classification access. Note, additional configuration combinations are possible.

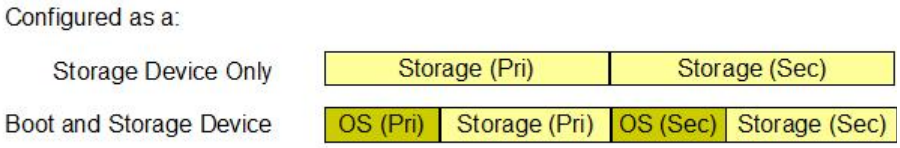


Figure 6: Conceptual Model (Dual Classification)

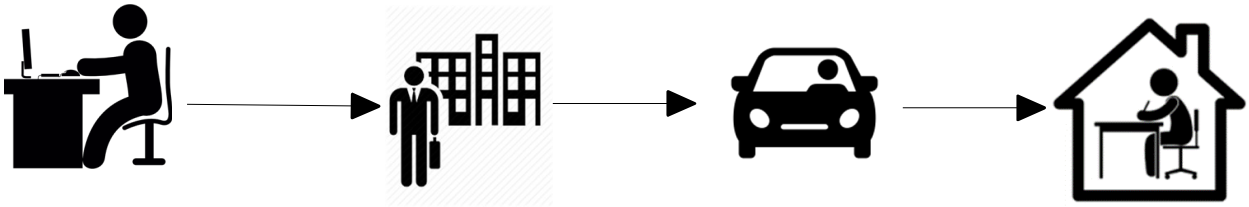
Typically the SDV-HA will be as a storage device that is accessed from a PC running Windows or as the first boot device for a PC where an OS, most likely Windows is booted from the SDV-HA.

During Initialisation the SDV-HA allows the creation of up to four data partitions for the primary storage area. This Initialisation partitioning function is provided to enable the SysAdmin 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. Partitioning of the secondary storage area, when enabled, is not provided during Initialisation.

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 possible by re-formatting the partitions in a native partition format for the operating system on which the SDV-HA will be used (e.g. NTFS on Windows).

USE SCENARIOS

Remote Working



The SDV-HA (with an operating system installed) is used with a diskless laptop outside of an agency's secure working environment. With approved high assurance communications equipment the remote laptop is used to connect to classified networks, but when powered-off the laptop and SDV-HA can be handled as PROTECTED.

Transportation of Highly Classified Data

The SDV-HA is used to transport highly classified data from one secure location to another. For instance, TOP SECRET data can be placed onto an SDV-HA in Canberra and the user can carry the device in a briefcase whilst travelling to the Australian Embassy in Washington.

Deployable Portable Secure Communications Pack

Several Defence and Government agencies utilise deployable portable communications packs in the form of a briefcase containing a diskless laptop, an SDV-HA containing a standard operating environment and secure communications equipment. These packs allow individuals to connect to classified networks from deployed locations, e.g. emergency relief operations or a military deployment.

Information Storage for Military C4ISR Systems

The SDV-HA is used to secure classified data in C4ISR systems.

TECHNICAL SPECIFICATIONS SDV-HA (HIGH ASSURANCE)

Product Identification

Product Name:	SDV-HA (High Assurance)
Model Number:	SDV-HAxxx
Hardware Model:	Rev 1 or Rev 2
Manufacturer:	Secure Systems Limited
Description:	Silicon Data Vault (SDV) secure high assurance portable data storage device.

Electrical Specifications

Input Supply Voltage:	5VDC +/-5%
Input Supply Current (Rev 1):	1.5A (maximum)
Input Supply Current (Rev 2):	3A (maximum)
Power Supply Source (Rev 1):	USB/eSATAp Host Interface
Power Supply Source (Rev 2):	USB Type-C Host Interface
Mean Time Between Failure (MTBF):	1 500 000 hours (excluding battery replacement every 4.5 years)

Mechanical

Enclosure Construction:	Aluminium Alloy
Enclosure Protective Coating:	Anodised Black OR Alodine/Powder Coating
Length (Rev 1):	143 mm
Length (Rev 2):	135 mm
Width:	81mm
Height:	20mm
Weight (Rev 1):	420 grams
Weight (Rev 2):	400 grams

External Interfaces

Host PC SATA Interface (Rev 1):	Combination eSATAp (1.5Gbps)
Host PC USB Interface (Rev 1):	Mini Type-B USB 2.0 (High Speed)
Host PC USB Interface (Rev 2):	Type-C USB 3.0 (SuperSpeed)
Token USB Interface:	Type-A USB 2.0 (Full Speed)
Status Indication:	Single Tri-colour status LED
Activity Indication (Rev 2):	Single blue activity LED

Storage Specifications

Secure Storage Capacity:	240, 480 and 960 GBytes
Host USB Vendor ID:	0x27B3
Host USB Product ID (Rev 1):	0x0100
Host USB Product ID (Rev 2):	0x0102

Security Specifications

Accreditation:	Australian Government High Assurance
Authentication:	Two Factor (Passphrase and Token)
Cryptography:	CNSA Suite Algorithms
Data Protection Level:	Up to and including TOP SECRET Classification

EMC/EMI Compliance

Radiated Emissions:	CISPR 32:2015 (RCM) 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

