SECURE SYSTEMS HIGH GRADE SILICON DATA VAULT

Product Description

The High Grade Silicon Data Vault (HGSDV) is a hardware product that can be used to reduce the storage and physical transfer requirements of data at rest through the use of data protection provided by the AES-128 cryptographic algorithm.

To log in to a laptop hosting a HGSDV a user must provide two factors of authentication – a password and an appropriate CD Token.

Evaluated Versions

The HGSDV is comprised of four major components. These are the firmware, the Authentication Application (AA), the System Administration Utility (SAU) and the CD Token Utility (CTU). The evaluated version of each component is listed below.

Component	Approved Versions
Firmware	2.0.5, or 2.0.4 in HDD or SSD versions
AA	1.1.0, or 1.0.9
SAU	4.1.0, or 4.0.9
CTU	3.0.2 only

The HGSDV version evaluated that corresponds to the component versions listed above is:

HGSDV Version	Part Number
SDV182A	SDV182A03MW3-nn-0104, or SDV182A03MW3-nnn-0105

Where "nnn" refers to the size of the integral storage device in gigabytes, e.g. 60 denotes a storage size of 60 gigabytes.

If a solid state disk drive (SSD) is present, the storage size will be suffixed with "S".

Scope of High Grade Evaluation

The scope of the High Grade Evaluation included the following security functionality:

- Identification and Authentication;
- Access Control;
- Secure Administration – an authenticated administrator can manage user accounts and

privileges and the product's configuration;

- Protection of Data – the product encrypts and decrypts data on the hard drive;
- Auditing; and
- Hardware and Business Processes.

If an Australian Government agency is considering using the High Grade Silicon Data Vault product they need to be aware that the following functionality was not included in the scope of the evaluation:

- the Add-on Product Module Activation feature;
- the Gatekeeper application;
- the Encrypted Back Up application; and
- the Remote Administration application.

DSD Findings - Summary

When the HGSDV is powered down, the HGSDV may reduce the handling requirements for classified material as follows:

- SECRET laptops can be stored and physically transferred as per UNCLASSIFIED FOR OFFICIAL USE ONLY requirements in the Protective Security Policy Framework (PSPF).
- CONFIDENTIAL and PROTECTED laptops can be stored and physically transferred as per agency guidelines for UNCLASSIFIED material.

Users must ensure that access to the device is controlled at all times.

Note: The storage and physical transfer requirements of TOP SECRET data at rest will not be reduced through the use of a HGSDV.

Key Management

CD Tokens used with the HGSDV must be seeded with trusted random data obtained from DSD. Australian Government agencies wishing to make use of an HGSDV must contact DSD to organise for the production and delivery of trusted random data to seed their CD tokens

Hardening Guide

For further advice with regard to setting up a laptop with a HGSDV to be as secure as possible, please see the *Laptop with High Grade Silicon Data Vault Hardening Guide* document available on the DSD Evaluated Product List (EPL).

PROTECT

Point of contact

For further information regarding the High Grade Silicon Data Vault's certification, cryptographic evaluation or compliance with the Information Security Manual (ISM), please contact DSD on 1300 CYBER1 (1300 292 371) or email assist@dsd.gov.au.

Secure Systems Limited may be able to provide alternative DSD-approved versions of this product on request. Please contact Secure Systems Limited on +61 8 9240 8708 or email secure@securesystems.com.au.

Date of this Consumer Guide

This Consumer Guide was updated by DSD on 8 March 2012.