



DSD'S CONSUMER GUIDE

## SECURE SYSTEMS' HIGH GRADE SILICON DATA VAULT PRODUCT

### 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 login into 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	Version
Firmware	2.0.4
AA	1.0.9
SAU	4.0.9
CTU	3.0.2

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

HGSDV Version	Part Number
SDV182A	SDV182A03MW3-nn-0104

Where “nn” refers to the size of the hard-disk drive in gigabytes, e.g. 60 denotes a hard disk size of 60 gigabytes.

### Scope of High Grade Evaluation

The scope of the High Grade evaluation included the following 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**

The HGSDV reduces the storage and physical transfer requirements of data at rest as follows:

- SECRET laptops can be stored and physically transferred as per RESTRICTED/X-IN-CONFIDENCE requirements in the Protective Security Manual (PSM);
- CONFIDENTIAL and RESTRICTED laptops can be stored and physically transferred as per agency guidelines for UNCLASSIFIED material.
- HIGHLY-PROTECTED, PROTECTED and X-IN-CONFIDENCE laptops can be stored and physically transferred as per agency guidelines for UNCLASSIFIED material.

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 at <http://www.dsd.gov.au/library/index.html#hardening>.

## **Point of Contact**

For further information regarding the High Grade Silicon Data Vault's certification, cryptographic evaluation or compliance with ACSI 33 please contact DSD on (02) 6265 0197 or email [assist@dsd.gov.au](mailto:assist@dsd.gov.au).

## **Date of this Consumer Guide**

This Consumer Guide was issued by DSD on 27 February 2009.