Secure Systems' Silicon Data Vault

Product Description

1. Silicon Data Vault (SDV) is a hardware product that provides protection of sensitive information on offline laptops and desktops. Protection is provided through pre-boot authentication and combined with hard disk encryption that is transparent to the user. Users should note that the SDV does not offer data protection once they are authenticated and local access is handled in the same way as remote access. This can potentially lead to unauthorised data access if the computer is networked.

Evaluated Version

2. The SDV is comprised of three major components. These are the firmware, the Authentication Application (AA), and the System Administration Utility (SAU). Both the laptop and desktop versions of the SDV have been evaluated. The evaluated version of each component is listed below:

Component	Desktop Version	Laptop Version
Firmware	1.3.8	1.6.2
AA	1.12	1.13
SAU	3.07A	3.07A

Common Criteria Certification - scope

3. The scope of the Common Criteria (CC) 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; and
   - Protection of Data – the product encrypts and decrypts data on the hard drive.

4. If an Australian government agency is considering using the Silicon Data Vault product then they need to be aware that the following functionality was not included as part of the product's functionality:

   - The Add-on Product Module Activation feature;
   - The Gatekeeper application;
   - Two-factor authentication; and
   - Remote administration.

5. Refer to the Silicon Data Vault certification report for the product's evaluated configuration and for recommendations regarding Australian and New Zealand Government users.

Common Criteria Certification – summary

6. The product has met the requirements of the Common Criteria evaluation assurance level to EAL 2.

DSD findings - summary

7. Because the product employs cryptography, DSD performed a cryptographic evaluation on the product in addition to the Common Criteria certification. The Silicon Data Vault uses 128-bit AES encryption.

8. Users are advised to select passwords of suitable length and type. DSD recommends passwords of length at least 12 characters with the requirement that the characters be drawn from upper case letters, lower case letters, numbers, and punctuation characters.

9. The product has been evaluated to EAL 2. As such, the Silicon Data Vault product can be used to reduce the storage and handling of the following information from:
   - IN-CONFIDENCE to UNCLASSIFIED;
   - RESTRICTED to UNCLASSIFIED;
   - PROTECTED to UNCLASSIFIED; and
   - HIGHLY PROTECTED to IN-CONFIDENCE.

Contact

10. For further information regarding the 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.

ACSI 33

11. The advice given in this document is in accordance with ACSI 33 release date March 2006. Australian government agencies are reminded to check the latest release of ACSI 33 at www.dsd.gov.au/library/infosec/acsi33.html to investigate if any changes have taken place.

Consumer Guide - date

12. This Consumer Guide was issued on 3 October 2006, by DSD.