



SECURE SYSTEMS LIMITED MINI AND POCKET SILICON DATA VAULT

Product Description

The Mini-SDV 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 authenticate to a Mini-SDV, a user must present their username and password.

Evaluated Versions

This Consumer Guide covers the following models from the Secure Systems SDV product range:

Model	Part Number	Description
Mini-SDV	SDV1M01-xxa / MU10	USB-connected external storage device
Pocket SDV	SDV4P06-xxa / P10	USB-connected external storage device

Scope of Evaluation

The scope of the DSD Cryptographic Evaluation (DCE) included the following security functionality:

- Pre-boot password based authentication;
- Post-boot password based authentication; and,
- Encryption of data

The scope of the DCE did not include the following security functionality:

- *Secure Operating Device* mode of operation

Common Criteria Certification – Summary

This product has not completed a Common Criteria Certification.

DSD Findings and Recommendations

DSD performed a DCE on the hardware, firmware and software components shared between the Mini-SDV and the Pocket SDV.

Although the DCE did not examine the *Secure Operating Device* mode of operation, this mode uses the same cryptographic functionality used by the *Storage-Only* mode. The *Secure Operating Device* mode of operation may be used with host equipment accredited to store and process information at the maximum classification of information stored on the Mini-SDV. The *Secure Operating Device* mode of operation must not be used with untrusted equipment.

Users are advised to select passwords of suitable length and type. DSD recommends passwords of at least 11 characters where characters are drawn from at least three of:

- Lower case letters;
- Upper case letters;
- Numbers; and,
- Symbols (such as punctuation).

If passwords are not drawn from three or more of the above sets, DSD recommends that passwords be at least 14 characters in length.

The Mini-SDV, when in a non-authenticated state and configured with an appropriate length password, can be used to reduce the handling requirements for data-at-rest as follows:

- UNCLASSIFIED (with Dissemination Limiting Markers) data handling requirements to UNCLASSIFIED
- PROTECTED (with Dissemination Limiting Markers) data handling requirements to UNCLASSIFIED

The Mini-SDV does not provide any protection to data stored on the device while it is in an authenticated state.

Point of contact

For further information regarding the Mini-SDV'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.

Date of this Consumer Guide

This Consumer Guide was issued by DSD on 1 February 2012.