

SECURE SYSTEMS Mini Silicon Data Vault (Mini-SDV[®])



Secure Systems Limited

SECURE STORAGE AND BUILT-IN SECURE BROWSER FOR TOTAL SECURITY REMOTE ACCESS

The Mini-SDV solves the problems that users have when wishing to securely access their data and corporate business applications whilst on the move. Combining AES on-the-fly hardware encryption with the ability to utilise a trusted browser or remote desktop client, securely loaded and stored on the device, the Mini-SDV provides a “secure laptop in your pocket”.



The Mini-SDV addresses a gap in the market and provides organisations with a cost-effective and convenient method of implementing a remote and mobile computing environment for teleworkers and mobile employees; it is aimed at organisations performing sensitive and high-value transactions over the Internet.

Packaged as a Universal Serial Bus (USB) attachable device, the integral trusted browser or remote desktop client is loaded into a (untrusted and potentially compromised) host PC's memory from a secure partition on the Mini-SDV and executed to enable secure access to web-enabled applications and perform remote data processing, securely.

Most portable storage devices are limited to using encrypted storage forcing users to “trust” that the applications they are using are not maliciously or accidentally leaving their sensitive data on the host PC.

With the Mini-SDV, these risks are addressed allowing users and organisations to safely and securely access applications and move large volumes of data without the cost, risk and inconvenience experienced in the past.

The Mini-SDV has been designed to address the following threats:

- *Malicious software capturing important credentials and data:* The ever increasing sophistication and proliferation of malicious software has made security-conscious organisations concerned about the integrity of PCs used by customers and/or employees for whom the organisation's PC security policy either does not apply or which may not be easily enforced.
- *Sensitive data traces remaining on a host PC's hard disk drive:* Upon the completion of a transaction, sensitive data remnants (in the form of temporary data/files) created by an application may remain on the PC hard disk drive unbeknown to the user.
- *Loss/theft of unsecured USB storage device:* Organisations are increasingly concerned about the use of unsecure USB devices to store ever larger volumes of sensitive information.

Secure Storage

Data encrypted on the fly during read and write operations.

Secure Browsing & Remote Access

Safely access your web-enabled applications and corporate network.

High-Capacity

Choose from 60Gb, 128Gb or 256Gb capacities.

Strong Authentication

Prevent unauthorised access to your data.

Access Control

Partition your data for separate users and/or separate secure



Mini SDV[®] - The Secure Laptop In Your Pocket



Technical Details

The Mini-SDV utilises the 'SDV chip', an application specific integrated circuit which sits in-line between a USB interface and the flash/solid state memory. The SDV chip allows partitions to be defined with Read-Only, Read-Write and No-Access permissions and provides cryptographically separated and controlled access to data. User profiles stored within the Mini-SDV define partition access rights. The Mini-SDV operates independently of the host PC's resources, providing encryption and decryption of all data transferred to and from the integral storage. The SDV chip includes a supervisory microprocessor, a data encryption engine, bus interface logic for direct connection to storage and USB interface logic.

The architecture and design of the Mini-SDV has in-built flexibility allowing future versions to implement additional features expected of a secure processing platform. These will include trusted operating systems and trusted applications such as office automation applications.

Technical Specification

Capacity – 60Gb, 128Gb or 256Gb

Dimensions – 81x70x12 mm

Weight – <70 grams

Security – Tamper Evident Enclosure

Choose from Two Operating Modes

The Mini-SDV can be used in one of two operating modes: "Fully Trusted" and "Assured", giving users the flexibility they need depending on the level of trust organisations have in the PCs to which they are connecting.

Used in **Fully Trusted** mode, the Mini-SDV provides users with the **ultimate secure operating platform**. In this scenario, a user plugs the Mini-SDV into an available USB port on the host PC and powers up. Once users have been successfully authenticated to the Mini-SDV, they are presented with the Mini-SDV's trusted browser or remote desktop client, through which they may securely access web-based applications on local or remote networks. In this mode, the user also has Read-Only access to the PC's hard disk drive.

The OS on the host PC is not used to execute any application and only the PC's memory and processor are utilised in this mode of operation. The Mini-SDV operates independently of the host PC's resources, providing encryption and decryption of all data transferred to and from the integral storage. The Mini-SDV also ensures that no data remnants are left on the host PC and the hardware enforced Read-Only partition on the Mini-SDV prevents any malicious software from attacking the trusted browser and the remote desktop client.

In **Assured** mode, the Mini-SDV provides a fast and convenient way of accessing the data and the trusted browser available on the device. In this scenario, upon plugging the Mini-SDV into a USB port on a host PC which has already booted the Windows OS, an authentication application is uploaded and auto-executed. Once successfully authenticated, the user has access to the Mini-SDV's storage. The hardware enforced Read-Only partition on the Mini-SDV prevents any malicious software from attacking the trusted browser and the applications and no data remnants are left on the host PC's hard disk drive.

Encryption – Dedicated AES hardware encryption chip

Security – Fully Trusted or Assured Modes of Operation

Interface – USB 2.0

Assurance – Based upon FIPS 140-2, DSD and Common Criteria approved technology



Common Criteria



FIPS 140 2 Validation

Secure Systems

8/152 Balcatta Road, Balcatta WA 6021

Tel: +61 (0)8 9240 8708

UNITRONIX Pty Ltd

PO Box 486, Morisset NSW 2264

NSW: Tel: 61 2 4977 3511 Fax: 61 2 4977 3522

WA: Tel: 61 8 9455 2424 Fax: 61 8 9455 2458

unitsyd@unitronix.com.au www.unitronix.com.au

www.securesystems.com.au