UNISYS

Unisys Stealth Solution for Secure Virtual Terminal

Stealth USB-Based Device

Unisys Stealth USB-Based Device

The Unisys Stealth™ USB-based device is a core component in an enterprise-class hardware, software and services solution that transforms the security of remote access. The Stealth Solution for Secure Virtual Terminal (SSVT) provides customized, dark network communications for authorized, authenticated users—avoiding security breaches which are complex and costly to resolve. SSVT is quickly provisioned, requires no application changes and facilitates security regulatory compliance.

Instead of booting from a client hard drive, SSVT provides protection by booting from a tamper proof, locked, virus-free operating environment, and safeguarding the transaction as it moves across the network. Stealth prevents malware from infiltrating the data by rendering the session undetectable on any network, and preventing interaction with any non-Stealth network activity and devices. Additionally, SSVT can be configured to eliminate data loss at the end user's PC/laptop.

Stealth Solution and Product Highlights

- Stealth Solution for Network Software is FIPS140-2, Level 1 certified
- SSVT USB Device is FIPS140-2, Level 3 certified
- Secure community of interest (COI) cryptographic access control
- Certified AES-256 encryption and SHA1/HMAC integrity enforcement
- Secure network data preventing loss, theft, misuse and corruption
- Protection of data-in-motion, ensuring confidentiality, integrity and availability
- Cloaking of Stealth-enabled devices
- Onboard malware protection
- Strong password authentication
- Tamper evident, waterproof and dust proof

Typical Deployment Scenarios

Many companies reactively deal with network security by monitoring their existing environment for viruses, Trojans and malware then removing them when discovered. SSVT is a comprehensive data protection solution that ensures an uncompromised internet business session through the use of a hardened, highly minimized operating system provided on the Stealth USB device, and a communications tunnel undetectable to everyone except those who are pre-identified as part of the "secure community" referred to as COI.

While most technologies focus on detecting and remediating attacks, SSVT safeguards organizations against the most challenging security risks by neutralizing existing infections and protecting the data as it is moving through the network. Simply put, SSVT allows users to securely work anywhere and leaves no trace of user activity on the system.

Typical scenarios for SSVT deployment:

- **Financial Service Institutions** – protects high value client online banking
- **Government or Enterprise Teleworkers** – provides secure, controlled access to organization assets
- **First Responder** – offers secure, portable access to agency servers; improves return time to command and control; and reduces cost of emergency infrastructure

Multiple SSVT Offerings

Stealth USB-based devices are currently Linux- or Windows-based, and may include an optional open partition with multiple GB capacity offerings. For more details, contact your local Unisys representative.

Stealth USB Device Specifications	
Features	• Optional secure open partition, varying capacity • Hardware-based AES-256 CBC mode encryption (FIPS Pub 197) • On-board malware protection • Strong password authentication • Zero software footprint • One year warranty
Operating Environments	• Linux (Ubuntu 9.10) or Windows embedded XP SP3 with IE7
Standards and Certifications	• FCC • CE • WEEE compliant • RoHS compliant
Physical and Electrical	• Compact and portable • Tamper-evident enclosure with removable cap • Durable, impact-resistant ABS plastic • Waterproof and dustproof to IEC 60529 IP57 • Waterproof enclosure to MIL-STD-810F • LEDs for power, data activity and authentication status • Uses USB bus power
Dimensions, Weight, Environmental	• Dimensions, Cap off: (H x W x L): 12.5 x 21.5 x 75 mm • Weight: 19g • Operating Temperature: {0 to 60 ℃} • Storage Temperature: {-20 to 70 ℃} • Relative Humidity: {5 to 95% non-condensing}

For more information, contact your Unisys representative or visit www.unisys.com/stealth

Specifications are subject to change without notice. ©2011 Unisys Corporation. All rights reserved.

The physical USB devices are supplied by Memory Experts International.

The Stealth Solution cryptographic module is FIPS 140-2 certified through the use of SecureParser® by Security First Corporation.

The software product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org)

The software product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

The software product includes software written by Tim Hudson (tjh@cryptsoft.com)

Printed in the United States of America 1/14