TRUSTED SYSTEMS
Security Made Simple

UserGuard

Desktop User Access Control System
Secures the Last 6ft to the Desktop
Targets the Insider Threat

"We take the leak out of Wiki"

USERGUARD FEATURES & BENEFITS

SECURITY FOCUSED ON NETWORK EQUIPMENT

- Devices housed in GSA approved Class 5 IPS Container
- Network devices remain in IPS Container and on-line 24/7
- Physical access to IPS Container and network devices restricted to admin/security personnel only

USER ACCESS RESTRICTED TO DESKTOP PERIPHERALS

- User authorized for network access, not network devices
- Two-factor authentication on desktop (CAC + PIN) connects user to network via KVM and Ethernet devices
- Local enrollment & admin from inside IPS Container
- Precedes & augments security of normal network logon

INSTANT SIPRNET ACCESS

- No boot up delays for anti-viral patch updates during logon
- Productivity & convenience enhanced with time savings

IMPROVED PERFORMANCE

- Simple, convenient security protocol encourages compliance, reduces OPSEC errors, neglect & avoidance
- Minimizes power cycling and rebooting, improving network stability and long term hardware reliability

SIMPLIFIED CONNECTIVITY & OPERATION

- Eliminates need for in-room PDS, conduit or drop boxes
- No off-line storage of hard drives, laptops or crypto keys
- No plugging or unplugging of devices for connectivity
- MultiGuard expansion flexibility for multiple users or single users access to multiple networks with one authentication

PERFECT BLEND OF SECURITY & CONVENIENCE

UserGuard was designed from the ground up for streamlined network access from the desktop without compromising security or network performance. It incorporates locally controlled two factor authentication (CAC & PIN) to connect the desktop KVM and Ethernet devices to the network. Once authorized, normal network logon proceeds with no interference with network traffic. UserGuard is comprised of two integrated modules, a Desktop Access Control Module, and an Intelligent Gateway mounted inside an IPS Container. The Desktop Access Control Module has a CAC reader, PIN pad, kill button and motion sensor activated disconnect. The Intelligent Gateway contains the I/O gateway controller module (HDMI/USB/Cat6), 8" tablet PC, USB/power control module and rack-mount tray with "whale tail" cable restraint.

IA/COMSEC teams are pleased, they control network devices, and users can't touch equipment. Users are pleased, no need to open the safe for access or deal with hardware. SCIFs and CAAs only protect space; IT/cyber security only protects the network, all reactive. Coupled with the IPS Container, UserGuard fills the void by proactively defending the network equipment and the access point, minimizing human intervention, simplifying security, enhancing performance, staying abreast of technological advances and emerging threats, keeping the insider out.

APPROVALS & ACCREDITATIONS

In the absence of Government standards covering the last six feet to the desktop, approvals have used the waiver process or through local DAA acceptance. Some progress has been made:

- JITC – Exemption - a physical security device with no DISN interaction
- DSS – Internal IA/COMSEC approval and accreditation
- DISA STIG – Group ID: V-31132, Rule ID: SV-41289r2 Version IA-12.01.01

TECHNICAL SPECIFICATIONS

Model Number: TSMSV1UGD-PC

Dimensions:
Intelligent Gateway: 1Ux11.75”D
Desktop Module: 2”Hx6.8”Wx10.3”D

Input Power: 100-240V, 50/60 Hz
Gateway: 1.0A, Desktop: 0.3A

CAC: Dedicated DoD approved or User Badge, HID RFID DoD approved reader

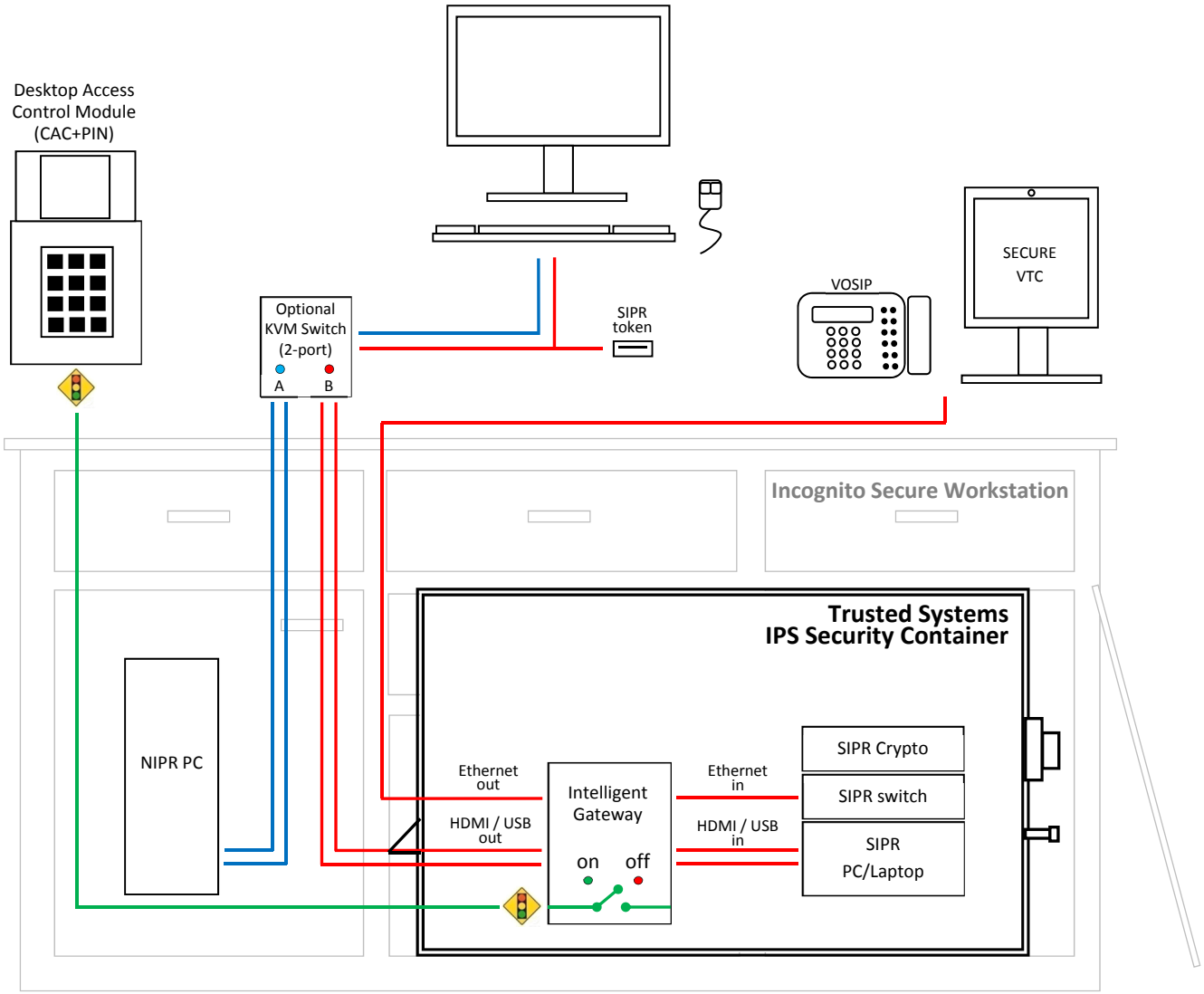
Authentication Software: 2FA

Processor: Dell 8” Tablet PC, Win 8.1 WiFi, Bluetooth, Camera deactivated

Standard Cable Sets:
Input: 6ft HDMI/USB/Cat6
Output: 15ft HDMI/USB/Cat6, USB hub

OPTIONS

- 30ft & 50ft output cable sets
- 2 or 4 Port KVM Switch with cables for SIPR, NIPR and/or other networks
- MultiGuard expansion module for multiple users or single user with multiple networks with single access



To activate the HDMI video, USB and Ethernet output to the desktop, the user places the pre-authorized CAC onto Desktop Access Control Module’s card reader and enters the corresponding PIN into the number pad. The user can now login to the network. When finished, just remove CAC from the card reader and system will disconnect. If the user walks away from the Desktop Access Control Module without removing the CAC, the system automatically times out via a motion sensor. The network can also be manually disconnected using the “Kill Button”.

Rev 03-2016

Trusted Systems, Inc.
(410) 756-3300
(800) 414-4203
www.trustedsys.com