



Product Highlights

- 📌 **Highest security by design** • the only desktop motherboard and PC that designed from scratch to serve as high-security device.
- 📌 **Hardware Based peripheral protection/isolation**
 - Absolutely no dependency on BIOS, OS or software applications. All peripheral protection functions are operating independently of all other functions. It can't be managed, disabled or upgraded.
- 📌 **Unidirectional optical data diodes** • used to secure USB peripherals isolation. Data can flow from devices to the PC only. No reverse data flow possible by physics.
- 📌 **Widest set of security functions** • Long list of security functions making this PC a unique solution.
- 📌 **Optional internal Secure KVM** • enables easy and secure connection of another desktop PC.
- 📌 **Support both PS/2 and USB peripherals with similar protection** • Highly-secured operation both with USB and PS/2 peripherals.
- 📌 **Cost effective** • this product was designed to provide an affordable solution for agencies and organizations. Cost reduction processes are taken to reduce production costs.
- 📌 **Anti tampering** • Always on active anti-tampering with 10 years battery. Special holographic tampering evident labels.

HSL Secure Desktop Overview

Have you ever wondered how it is possible that kids in the kindergarten using the same PCs that the CIA employees are using? Strange isn't it? One size fits all? What about security? In the new world of networking and cyber attacks, commercial PCs are the wrong machine for the job (if your job deals with classified data). There is a worldwide need and effort to develop desktop PCs that will provide much better protection compared to commercial PCs.

Although the changes needed are very fundamental, the effort in developing such platforms is to make them affordable (cost wise) and compatible with existing networks, Operating Systems and applications. HSL is working hand in hand with some key customers worldwide in an effort to develop a secure desktop that will answer these customer's specific needs.

HSL's Secure Desktop is not about TEMPEST and electromagnetic emissions – these are not the primary threats today. It is also not the security “patch” offered by TPM or other add-on modules. Primary threats today are infected networks, software and the internal (trusted) users. HSL Secure Desktop relies on the latest hardware / firmware security tools to protect the desktop PC from wide range of threats. Most of these tools are operating before BIOS (or UEFI) is even loaded and run.

One of the key challenges in this project is the timeframe. It takes few years to develop test and certify a platform like this. It typically takes 1 year for a PC platform to become obsolete as the technologies involved are changed rapidly. HSL addressed this challenge by developing a set of fully tested and evaluated protection tools that can be easily implemented on the target motherboard and enclosure. This method reduces the time to market of a Secure Desktop and still provides the best set of protection means.

HSL designed an internal Secure KVM option to add another layer of security to this product and to provide an integrated solution for the secure user desktop.

Secure Desktop Specification	
CPU	<ul style="list-style-type: none"> ▪ AMD "Fusion" G Series dual-core CPU 1.66 GHz ▪ 64KB of L1 cache, plus 512KB of L2 cache per processor core ▪ Supports Secure Virtualization
Memory & storage	<ul style="list-style-type: none"> ▪ Memory - 4 GB DDR3-1333 ▪ Storage – SATA Disk On Module Solid State Disk. 2.5" SSD or HDD [optional]
Peripheral ports	<ul style="list-style-type: none"> ▪ 1 x USB Type-A receptacle to connect user mouse (filtered by hardware) ▪ 1 x USB Type-A receptacle to connect user keyboard (filtered by hardware) ▪ 1 x USB Type-A receptacle to connect user authentication device (filtered by hardware) ▪ 1 x input 3.5 mm jack to connect a microphone [optional] ▪ 1 x output 3.5 mm stereo jack to connect headphones
LAN	<ul style="list-style-type: none"> ▪ 1 x RJ-45 jack for LAN connectivity supporting 10/100/1000 Base-T Ethernet ▪ 1 x SFP cage to connect fiber transceiver module supports: 100 Base-FL, 1000 Base-FX and 1000 Base SX [optional] ▪ Wake on LAN support
Video	<ul style="list-style-type: none"> ▪ Graphics AMD Radeon™ HD 6320 with 80 graphic cores ▪ Dual independent displays support ▪ DisplayPort output supports resolutions up to 2560x1600 (optional Dual DP output) ▪ DVI-I output supports resolutions up to 1920x1200 Digital or 2560x1600 Analog (VGA) ▪ 3D Acceleration <ul style="list-style-type: none"> • Full DirectX® 11 support, including full speed 32-bit floating point per component operations. • Shader Model 5 • OpenCL™ 1.1 support • OpenGL 4.0 support ▪ Dedicated hardware (UVD 3) for H.264, VC-1 and MPEG2 decode
Operating system and firmware	<ul style="list-style-type: none"> ▪ Microsoft Windows 7 / Windows 7 Embedded ▪ Security enhanced Linux based kernel ▪ VMware Workstation 7 ▪ Can be configured as thin-client with Browser, Citrix and RDP support only.
Power	<ul style="list-style-type: none"> ▪ Internal universal power supply ▪ Input voltage 90-240VAC DC to 400 Hz ▪ 40W power consumption maximum ▪ 28VDC Power option available
Physical Characteristics	<ul style="list-style-type: none"> ▪ Dimensions: 60 (W) x 210 (D) x 300 (H) mm / 2.36 (W) x 8.27 (D) x 11.81 (H) inch ▪ Device weight: 2.75 Kg. (6.05 lbs.) ▪ Shipping Weight: 3.4 Kg (7.5 lbs) without cables
Security Features	<ul style="list-style-type: none"> ▪ Motherboard and enclosure specifically designed for high-security applications ▪ TEMPEST Enclosure and power filters SDIP-27 Level B standard. Level A [optional]

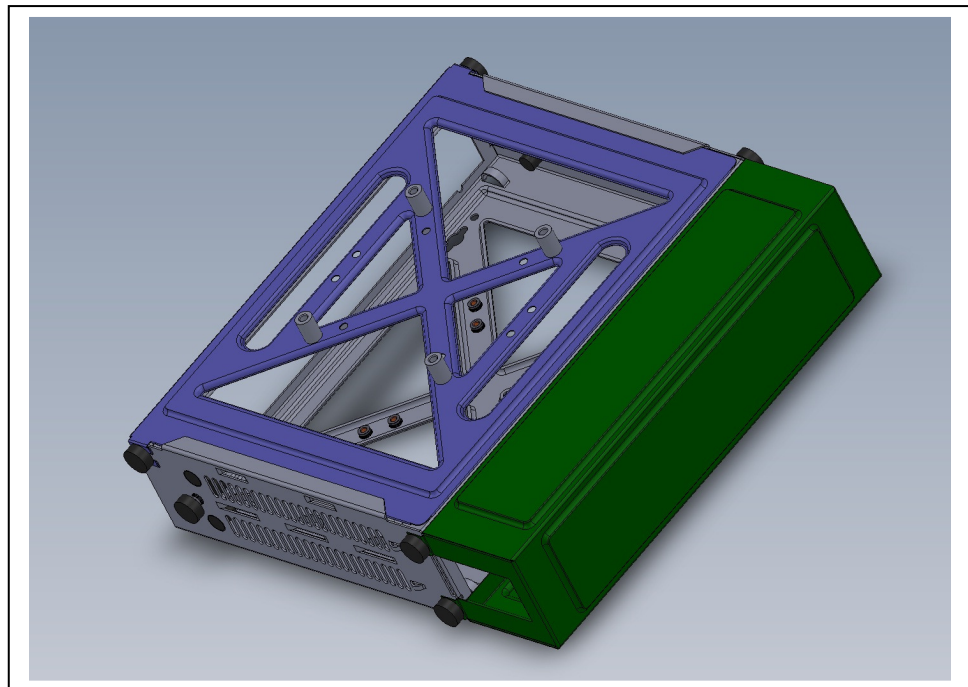
	<ul style="list-style-type: none"> Keyboard USB port is emulated, filtered by hardware and have uni-directional optical data diode to protect from data leakages. Mouse USB port is emulated, filtered by hardware and have uni-directional optical data diode to protect from data leakages. User authentication port is filtered, emulated and monitored by hardware. Hardware based disk encryption support AES-256 or custom algorithms. Keys not accessible to host. Advanced active anti-tampering system with back-up battery to detect physical intrusion attempts. Disables the computer if tampering detected, erase keys and log events in crypto memory. Keys stored in crypto memory device with protection from freezing, under and over voltage, side-channel attacks, die de-capsulation etc. Strong device authentication using non-standard TPM No BIOS – boot-loader stored on ROM chip to prevent attacks. Custom built UEFI with no user settings and no NVRAM or RTC registers. 100% o Boot-loader and UEFI source code available for audit. Holographic Tampering Evident Labels to detect enclosure tampering. IP Traffic encryption using hardware crypto module. Radiated and conducted emission filters on all I/O and power lines. Display EDID is emulated and filtered by a firewall in hardware to prevent EDID attacks. Audio CODEC can be physically disabled by a special switch. Hot microphone indicated by illuminated light (LED). Product delivered to customer in factory-sealed container to prevent tampering while in transit. No exposed or internal unused ports or connectors. Extremely low emissions due to low power consumption (less than 40W). Support fiber LAN and fiber KVM extender to remote display to reduce cable emissions. Optional Emergency Switch to sanitize the computer (all keys and local files are erased). Stainless steel security cage available to lock the device and all connected cables.
Optional Secure KVM module	<ul style="list-style-type: none"> 2 Ports 3rd-Generation Secure KVM Complies with Common Criteria EAL-4+ NIAP Peripheral Sharing Device Protection Profile 2.1 Channel switching is done through keyboard shortcuts Supports DVI-I (including VGA), USB keyboard and mouse, USB user authentication device and stereo audio out. Optical data diodes to prevent peripheral leakages.
Security Accreditation	<ul style="list-style-type: none"> Common Criteria EAL 4+ pending, Secure Desktop Computer 1.1 Protection Profile. TEMPEST NATO / US Pending
Environmental	<ul style="list-style-type: none"> Temperature range: Operating - 0°C to 40°C (32°F to 104°F); Storage - -20°C to 60°C (-4°F to 140°F) Humidity: Operating - 20 to 80% non condensing; Storage – 10 to 90% non condensing Altitude: 0 to 10,000 ft
Certification	<ul style="list-style-type: none"> CE UL and cUL EMI/EMC: FCC Class B, CE Mark, EN55022B, VCCI Safety BSEN60950 / EN60950

- Specifications are subjected to change without prior notice
- Multiple patents pending

HSPC800 Internal shielding enclosure



Stainless Steel Security Cage



How to Order

Models

Description	Part Number
HSPC801 – Secure Desktop Computer, AMD G-Series CPU, Dual Core 1.66 GHz, 2 GB DDR3, 4GB SATA DOM, TEMPEST SDIP-27 Level B / USA NSTISSAM Level II, Windows 7 Embedded OS	CPN06057
HSPC822 – Secure Desktop Computer, AMD G-Series CPU, Dual Core 1.66 GHz, 2 GB DDR3, 4GB SATA DOM, TEMPEST SDIP-27 Level B / USA NSTISSAM Level II, Windows 7 Embedded OS with internal 2 ports Secure KVM	CPN06058

Cables (needed only when internal Secure KVM is in use)

Description	Part Number
KVM Cable short (1.8 m), DVI-D to DVI-D Single-Link, USB, Black	CPN05485
KVM Cable short (1.8 m), DVI-D to DVI-D Dual-Link, USB, Black	CPN05486
KVM Cable short (1.8 m), DVI-A to VGA, USB, Black	CPN05489
KVM Cable short (1.8 m), Audio out, CAC, Black	CPN05490

Accessories and spare parts

Description	Part Number
SCM Smart-card reader, USB, SCR-3311	CPN05498
HSPC8xx Secure Cage	CPN06059

Services

Description	Part Number
HSPC8xx 1 Year Standard warranty and support extension (3rd to 7th year) per S/N	HSV06060
HSPC8xx 1 Year Premium warranty and 24/7 support per S/N	HSV06061