ORWL

Present Key

[ORWL]

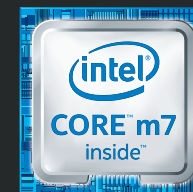CES INNOVATION AWARDS 2016 HONOREE

intel CORE™ m7 inside™

MEET ORWL

- Tamper Proof Secure Workstation
- Two Factor Authentication
- User Presence Control

- Self Encrypting SSD
- Enable Single Sign-On
- Motion Sensor

- Designed for Windows and Linux
- Side Channel Protection
- Ready for Virtualization

[ORWL], A POWERFUL WORKSTATION.

[ORWL] is a new category of secure workstation bringing you the utmost security technologies to protect your data. It requires both a physical key and a password to be used. [ORWL] secure workstation is a secure endpoint to control access to your cloud services, as part of a secure network. It can also replace any computer thanks to its built-in security.

Privacy is at the Core of Security

Privacy consists in the combination of privacy of data, privacy of communication and privacy in society. Thanks to its security-focused design, [ORWL] take care of all aspects of privacy: its SSD hard disk is encrypted, its communication ports are controlled and will be shut down in response to any attack, and each [ORWL] is unique.

Security is as Good as the Weakest Link in the Chain

Thanks to its hardware architecture, [ORWL] brings state-of-the-art authentication and high-end security technologies to the secure workstation. It delivers physical, bank-level information security for everyone.

> **" IF YOU SPEND MORE ON COFFEE THAN ON IT SECURITY, YOU WILL BE HACKED. WHAT'S MORE, YOU DESERVE TO BE HACKED. "**
>
> White House Cybersecurity Advisor, Richard Clarke

[ORWL] adds two-factor boot authentication to a compact, portable secure workstation. That means you need both a physical key and a password just to power [ORWL] on. Keyfobs are generated with a secure procedure making each [ORWL] unique. They are not duplicated.

A secure microcontroller subsystem controls the power. You can't hack what is not on.

A New Category of Secure Workstation

[ORWL] comes with two unique wireless access keyfobs that are required to switch on the device and boot. [ORWL] embedded security controls all accesses: Networks, Bluetooth, Wifi, USB ports, HDMI,... [ORWL] will lock if its authorized user is out of a 10 meter range and will shut down if moved while unattended.

If any of the six external tamper sensor is triggered, [ORWL] will erase the SSD encryption key, erase all access credentials and prevent the unit from restarting.
[ORWL] has been designed with security and reliability in mind. Its MTBF is higher than a million hours.
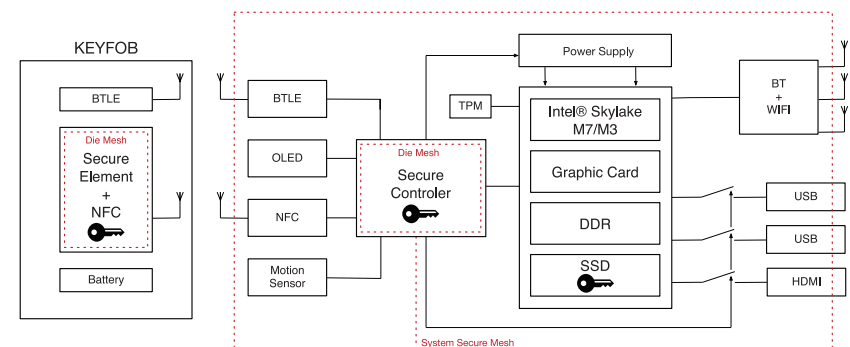
A Powerful Secure Workstation

[ORWL] includes a PC base and runs the latest X86 Intel® processor architecture 'Skylake' Y Core™ M. [ORWL] is available in 2GB or 8GB DDR3 and 120GB to 480GB SSD drive. Two controlled USB ports will connect power, keyboard and mouse. A micro-HDMI output will display up to 4k video with audio.

[ORWL] provides authentication and encryption thanks to its hardware accelerator. [ORWL] integrates a secure IEEE 802.11AC 2×2 Dual Band, and BT 4.2, access point, so that you can connect to other devices and networks wirelessly.

[ORWL] supports Bare Metal virtualization, thanks to Intel® VT-x and IOMMU VT-d. You can run a VM-based OS. [ORWL] is designed according to Open Source principles making its components available to third parties.

[ORWL] benefits from remote IT support allowing to securely bring assistance to IT managers. [ORWL] has been designed with security and reliability in mind. Its MTBF is higher than a million hours.

TECHNICAL SPECIFICATIONS

Intel® Skylake Y	• Includes Intel® HD graphics 515 300/1000 MHz	
Core™ M5 6Y54	• 2 cores/4 threads 900 MHz, 4MB L3 cache • 2 GHz single core turbo, 2.2 GHz dual core Turbo, includes VT-d, VT-x and AES-NI	
Core™ M7 6Y75	• 2 cores/4 threads 1.2GHz, 4MB L3 cache • 3.10GHz single core turbo, 2.9GHz dual core Turbo, includes Intel VPro, TXT, VT-d, VT-x and AES-NI	
LPDDR3	• 8GB @1600 MHz, Max Bandwidth 25GB/s	
SSD	• SSD 120GB to 480GB • NGFF-2280, M.2 type	• SATA Gen.3, 6Gbps • MTBF: ≥1 million hours
WLAN	• Intel® Wireless • IEEE 802.11 a/b/g/n/ac, Dual band, 2×2 • Dual Mode Bluetooth® 2.1, 2.1 + EDR, 3.0, 4.2 (BLE)	
TPM	• Compliant to TPM 2.0 Rev. 0.9x • LPC interface 24/33MHz	• FW "upgradable" to TPM 2.0 • TIS 1.3
Accelerometer	• Six-Axis (Gyro + Accelerometer) MEMS Motion Tracking Device, InvenSense MPU-6500	
Secure element	• Secure Boot Loader with Public Key Authentication • AES, DES and SHA Hardware Accelerators • Modulo Arithmetic Hardware Accelerator (MAA) Supporting RSA, DSA and ECDSA • Hardware True Random-Number Generator • Die Shield with Dynamic Fault Detection • 6 External Tamper Sensors with Independent Random Dynamic BIT Patterns circulated for protection • 256-Bit Flip-Flop-Based gateway providing on the fly encryption and decryption of data for Battery-Backup SRAM. Destructive reset signal to reset of this flip flop on internal or external tamper • Frequency, Temperature and Voltage Tamper Monitor • Real-Time Clock	
NFC reader	• Read/write mode supporting ISO/IEC 14443A/MIFARE	• Read/write mode supporting ISO/IEC 14443B
Secure Display	• 1.5 inch White OLED display	
Ports	• 2× USB Type C, supporting power delivery and Display Port (DP) output • 1× Micro HDMI 1.4, up to 4K resolution	
Keyfob	• Each unit comes with two NFC keyfobs to be paired by the owner	• Additional keys can be purchased
BT Beacon	• BLE 4.1 Beacon with pedometer for proximity estimation and protection	
NFC + Secure element	• ISO/IEC 14443 Types A and B, ECMA 340 (NFCIP-1), in Card Emulation mode • Switching between operating modes and RF modes • NCI functions for Device Host link	
Size	• Ø128 mm × 31.4 mm (Glass version)	
In the box	• 1× ORWL, 2× KEYS, HDMI cable, power supply, USB cable	

Design SHIFT