



solutions for trusted computing  
solutions for trusted computing



Commercially Proven Trusted Computing Solutions

RSA 2010

# Hardware Self-Encrypting Drives (SEDs)

- **Unique Security Features**
  - ❑ Encryption below the file system
  - ❑ Hardware root-of-trust for encryption
  - ❑ Tamper resistant packaging
- **Unique Compliance Feature**
  - ❑ Hardware root-of-trust for management
- **Unique usability Features**
  - ❑ Always encrypting architecture
- **Management Best Practices**
- **TPM Capabilities & Usage**



# SED: Commercially Successful Trusted Computing Solution

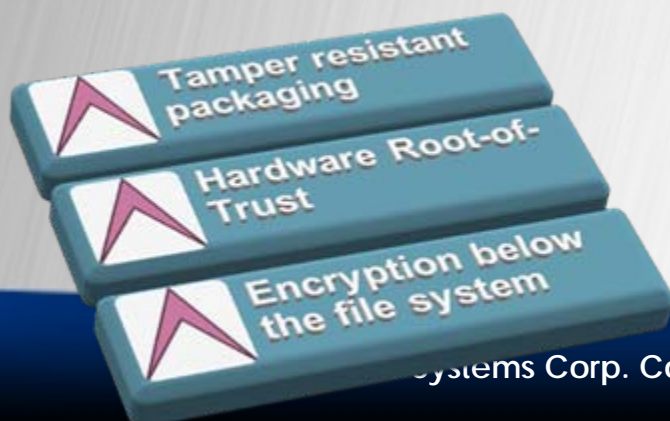
## WHY

- **Best-in-Class Security**
  - Embedded & Robust
- **Ease of Management**
  - Central Control & Local Autonomy
- **Ease of use**
  - Transparent & Responsive
- **Supply Chain alignment**
  - HDD Vendors, ISV, PC OEMs, Customers
- **Standards based**



# SED Unique Data Protection Attributes:

- Encryption module is embedded in the drive hardware
  - ❑ SED partition table and the file system are encrypted
  - ❑ Reduced Attack surface, especially off-line attack
- Encryption module has embedded management & access control functions
  - ❑ Provides a hardware Root-of-Trust for encryption
  - ❑ 'Always-Embedded' key management effectively adds 2-Factor data protection
  - ❑ **Factor 1:** Drive access credentials      **Factor 2:** Encrypting hardware with embedded key
- Tamper resistant features in the embedded packaging
  - ❑ e.g. Simple lockout latch can force a power-cycle after 5 consecutive failed auth attempts
  - ❑ Power-cycle delay makes a password attack impractical



**SED**  
3 separate layers of security  
integrated in a single  
embedded hardware module

# SED Unique Secure Management Attributes:

- Hardware embedded User & Administrator roles
  - Hardware “Root-of-Trust” for management
  - Embedded strong authentication for management access
  - **Enables exclusive remote ownership of management functions**
- Server is exclusive proxy owner of all drives
  - Unique strong management credentials required for each drive
  - Single point of management for all drives
  - **No local admin or user can modify/disable security settings**
- Secure centralized log of all management actions
  - **Forensic legitimacy**



## Hardware Root-of-Trust for encryption management

Forensically complete & legitimate record of all management actions  
in case of PC loss or theft

# SED Unique Ease-of-use Attributes

- Hardware embedded encryption is “Always On”
  - ❑ “Always Encrypting” even when “Drive Locking” is disabled
  - ❑ “Drive locking” ENABLED imposes hardware embedded access control on the Encryption key
  - ❑ **Switching to “encryption-on” is instantaneous. No lengthy data conversion**
- Below the file system encryption does not impact OS patch operations
  - ❑ **No decryption/encryption necessary on OS patches & upgrades**
- SED usability features
  - ❑ **Embedded encryption operates at media speeds - no performance hit**
  - ❑ **Pre-boot intelligence to support secure Windows SSO & WPS**
- Hardware embedded encryption is transparent
  - ❑ Reduced management and support overhead
  - ❑ **Embedded form factor puts enterprise-class data-protection in the reach of the SMB / SOHO**
  - ❑ **Factory integrated – Unified Support**



# SED Management: Best Practices

- “Always Embedded” key management architecture
- Exclusive server based ownership of all SED management privileges
  - Disable local management
- Tamper evident central audit logs
- Role based fine grained authorization of server administrative functions
  
- Plus standard usability features

SSO  
WPS  
Pre-boot log  
Helpdesk  
Auto-provisioning

S3/S4 Support  
Logging / Query  
Alerting / Alarm  
Reporting  
AD / MMC integration

External Drives  
Clients outside the firewall  
Foreign Clients (Non-domain)  
Scripting  
Crypto-Erase

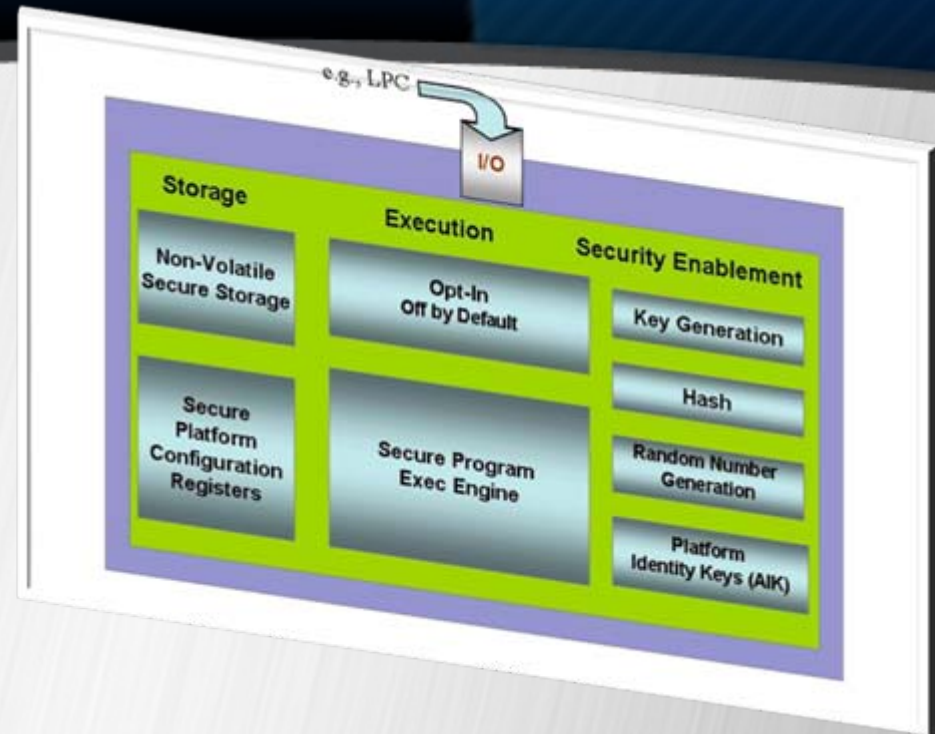
ETC,

ETC,

ETC

# TPM security attributes:

- Trusted Platform Module (TPM)
  - ❑ OS Independent Cryptography
  - ❑ Hardware “Root-of-Trust” for Storage
  - ❑ Hardware “Root-of-Trust” for Management
  - ❑ **Tamper resistant packaging**
- Hardware embedded SmartCard Apps
  - ❑ Interoperable with Microsoft CA
  - ❑ Interoperable with Kerberos
  - ❑ **Strong Authentication: The PC is the token**
- Software CSPs have been compromised
  - ❑ **Jailbreak tool coupled with local admin rights can enable impersonation**
  - ❑ **TPM protects with Hardware embedded security**
  - ❑ **Secure Authorization & Signing for all types of Applications**
    - ❖ VPN, Wi-Fi, Kerberos, Signing, S-Mime,
    - ❖ SAAS SSO / Federation



# Summary

- Unique Security features
  - Encryption is below the file system
  - Hardware root-of-trust for storage
  - Tamper resistant packaging
- Unique Compliance feature
  - Hardware root-of-trust for management
- Unique usability features
  - Always encrypting architecture
- Management Best Practices
- TPM capabilities & Usage

**Come  
Visit  
Wave at  
Booth  
#1849**