

Where Is Your Data Tonight? A Lesson in Avoiding Fines, Headlines or Worse

Copyright © Trusted Computing Group

InformationWeek
WEBCAST

Where is Your Data Tonight? A Lesson in Avoiding Fines, Headlines or Worse

An InformationWeek Webcast

Sponsored by Trusted Computing Group

UBM
TechWeb

Today's Presenters

Paul Korzeniowski, Contributing Editor, Information Week

Dr. Michael Willett, Storage Security Strategist, Samsung

Mike James, Director of SoC Development, Toshiba

Challenges That IT Departments Face



Paul Korzeniowski
Information Week

UBM TechWeb

Data Deluge

- Companies generating more data
- More end user devices
- More competition
  - More analytics
- More data complexity



More Data, Less Security

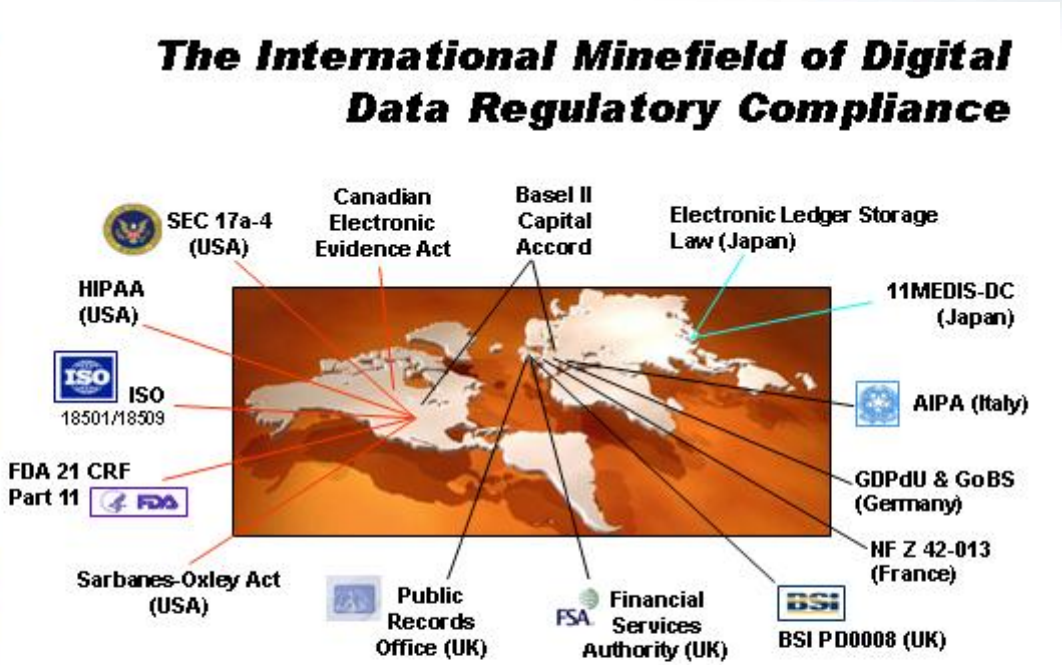
- More data generated , more chances for intrusion
- 345,124,400 records have been breached since 2005
- Organized Crime's role
- $6.65 million per affected corporation ($202 per record)



Increase in Government Regulations



The Archival Storage Challenge



- 10,000 regulations in US alone
- Scope: Compliance with Federal, State and Local regulations
- Depth: Industry-specific, public corporations
- Impact: Cost to comply or remediate, penalties for non-compliance

UBM TechWeb

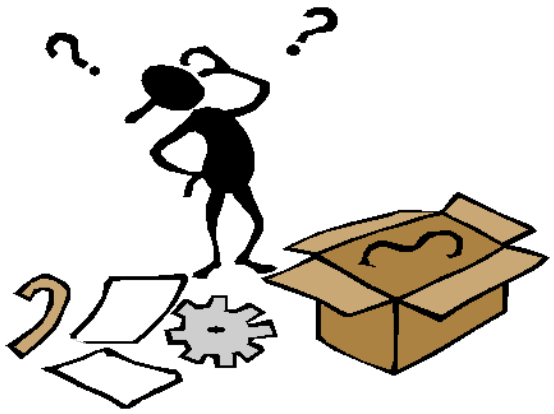
Current Data Security Constraints

- Increased system complexity
- Lower budgets
- Balance security risks versus security investments



Data Security Needs

- Inexpensive
- Comprehensive
- Easy to deploy
- Works with a broad of systems



Self-Encrypting Drives

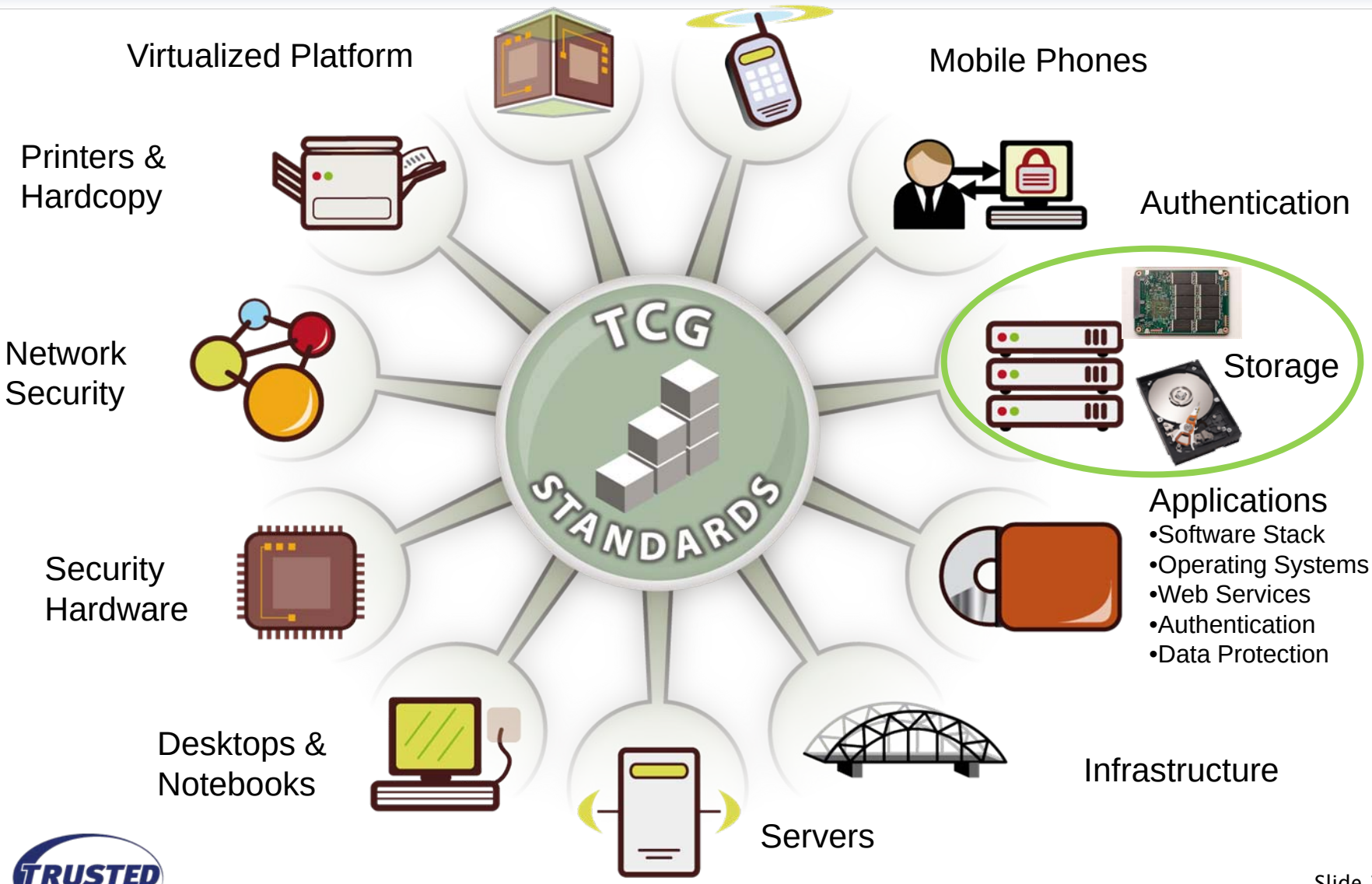
BENEFITS and PERFORMANCE

Dr. Michael Willett, Samsung

TRUSTED COMPUTING GROUP™

Trusted Computing Group Confidential

Complete Trusted Enterprise Solutions



Copyright© 2010 Trusted Computing Group.

Why Encrypt Data-At-Rest?

Threat scenario: stored data leaves the owner's control – lost, stolen, re-purposed, repaired, end-of-life, …



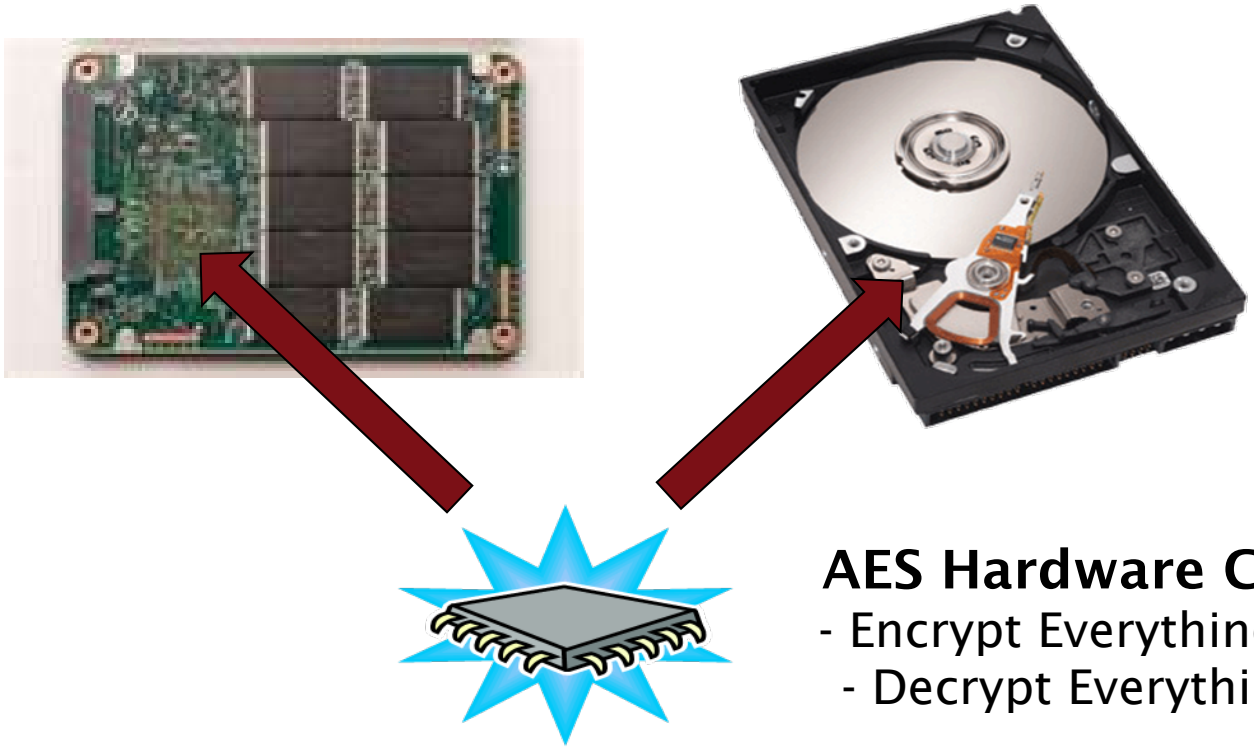
- Compliance
  - 46+ states have data privacy laws with encryption safe harbors
  - New data breach bills have explicit encryption safe harbors
- Data center and laptop drives are mobile (HDD, SSD)
- Exposure of data loss is expensive ($6.65 Million on average per incident[1])
- Obsolete, Failed, Stolen, Misplaced…
  - Nearly ALL drives leave the security of the data center
  - The vast majority of decommissioned drives are still readable

1. Ponemon Institute, Fourth Annual US Cost of Data Breach Study – Jan 2009 www.ponemon.org

Copyright© 2010 Trusted Computing Group.

What Is a Self-Encrypting Drive (SED)?

Trusted Computing Group
SED Management Interface



AES Hardware Circuitry
- Encrypt Everything Written
- Decrypt Everything Read

Copyright© 2010 Trusted Computing Group.

Self-Encrypting Drives

- Simplified Management
- Robust Security
- Compliance "Safe Harbor"
- Cuts Disposal Costs
- Scalable
- Interoperable
- Integrated
- Transparent

"Many organizations are considering **drive-level security for its simplicity** in helping secure sensitive data through the hardware lifecycle from initial setup, to upgrade transitions and disposal"

Eric Ouellet
Research Vice President
Gartner

Copyright© 2010 Trusted Computing Group.

‘Hurdles’ to Implementing Encryption…

Key management/data loss	• Tracking and managing encryption keys • Tracking and managing authentication keys (passwords for unlocking drives)
Complexity	• Data classification • Impact on OS, applications, databases • Interoperability
Performance	• Performance degradation; scalability
Cost	• Initial acquisition costs • Deployment costs

TRUSTED COMPUTING GROUP™

Copyright© 2010 Trusted Computing Group.

Hardware-Based Self-Encryption versus Software Encryption

- **Ease of Deployment:** Encryption key generated in the factory
- **Transparency:** Once unlocked, functions as a regular drive
- **Ease of management:** No encryption key to manage
- **Life-cycle costs:** Lower initial and on-going costs
- **Disposal or re-purposing cost:** With an SED, erase on-board encryption key
- **Re-encryption:** With SED, there is no need to ever re-encrypt the data
- **Performance:** No degradation in SED performance
- **Standardization:** Whole drive industry is building to the TCG/SED Specs
- **No interference** with upstream processes

ISSUE: Hardware acquisition (part of normal replacement cycle)

Copyright© 2010 Trusted Computing Group.

Software versus Self-Encryption: Performance Comparison

Performance Throughput Tests

	No Encryption	Seagate Self-Encrypting Drive	Software Encryption Average	Software Product 1	Software Product 2	Software Product 3
Startup Throughput (MB/second)	7.90	**7.99**	7.73	7.87	7.80	7.53
Application Loading (MB/second)	**5.89**	5.71	5.51	5.63	5.50	5.40
Modest Size File Test (MB/second)	**5.40**	5.28	5.14	5.11	5.20	5.10
Extensive Data Read (MB/second)	80.20	**82.75**	38.57	46.27	35.60	33.84
Extensive Data Write (MB/second)	**50.65**	50.31	35.15	39.14	31.40	34.90

System Startup/Shutdown Effects

	No Encryption	Seagate Self-Encrypting Drive	Software Encryption Average	Software Product 1	Software Product 2	Software Product 3
Startup Time (seconds)	37.10	**34.47**	47.24	41.49	52.02	48.22
Shutdown Time (seconds)	11.97	**11.79**	17.90	12.03	29.29	12.37
Hibernate Time (seconds)	29.16	**28.62**	31.14	28.71	29.61	35.1
Hibernate Recover Time (seconds)	**21.42**	23.22	40.80	26.37	41.26	54.76

http://www.trustedstrategies.com/papers/comparing_hardware_and_software_fde.pdf

TRUSTED COMPUTING GROUP™

Copyright© 2010 Trusted Computing Group.

Addressing the Hurdles…

Simplifies Key Management to Prevent Data Loss	✓ Encryption key does not leave the drive; it does not need to be escrowed, tracked, or managed
Simplifies Planning and Management	✓ Standards-based for optimal manageability and interoperability ✓ Transparent to application developers and database administrators. No change to OS, applications, databases ✓ Data classification not needed to maintain performance
Solves Performance	✓ No performance degradation ✓ Automatically scales linearly ✓ Can change keys without re-encrypting data
Reduces Cost	✓ Standards enables competition and drive cost down ✓ Compression and de-duplication maintained ✓ Simplifies decommissioning and preserves hardware value for returns, repurposing

TRUSTED COMPUTING GROUP™

Copyright© 2010 Trusted Computing Group.

Self-Encrypting Drives
TECHNOLOGY

Mike James, Toshiba

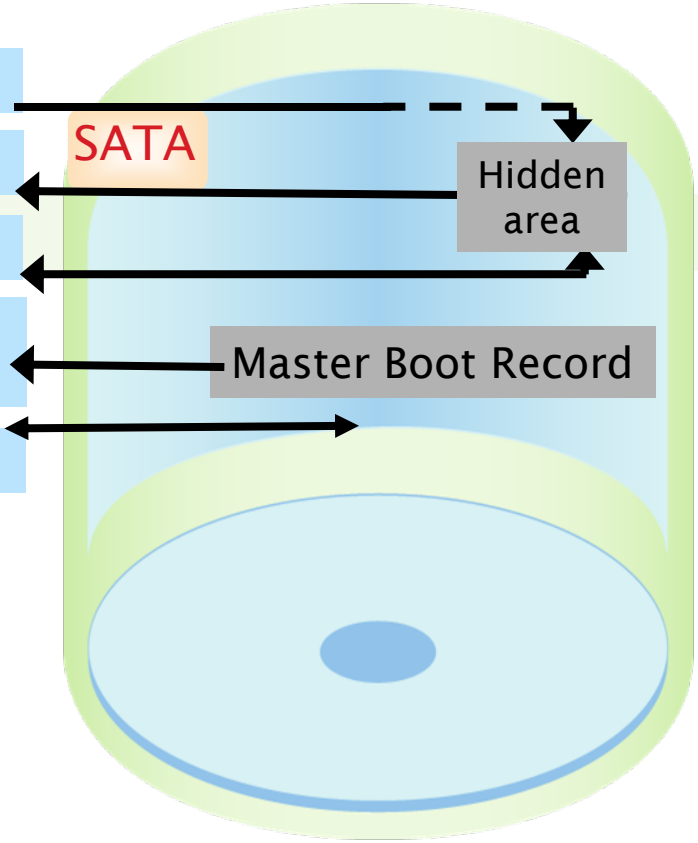
TRUSTED COMPUTING GROUP™

Trusted Computing Group Confidential

Booting a SED in a Laptop or Desktop PC

- At boot time (when power is turned on), the drive is locked and encryption keys are not available to the drive
- The Pre-Boot Authentication code is presented to the PC with the following method:

1. BIOS attempts MBR read; drive redirects to pre-boot area
2. PC loads pre-boot OS from Drive
3. User enters authentication credentials for drive to verify
4. If authentication successful, drive unlocks and boots original MBR
5. Normal operation commences

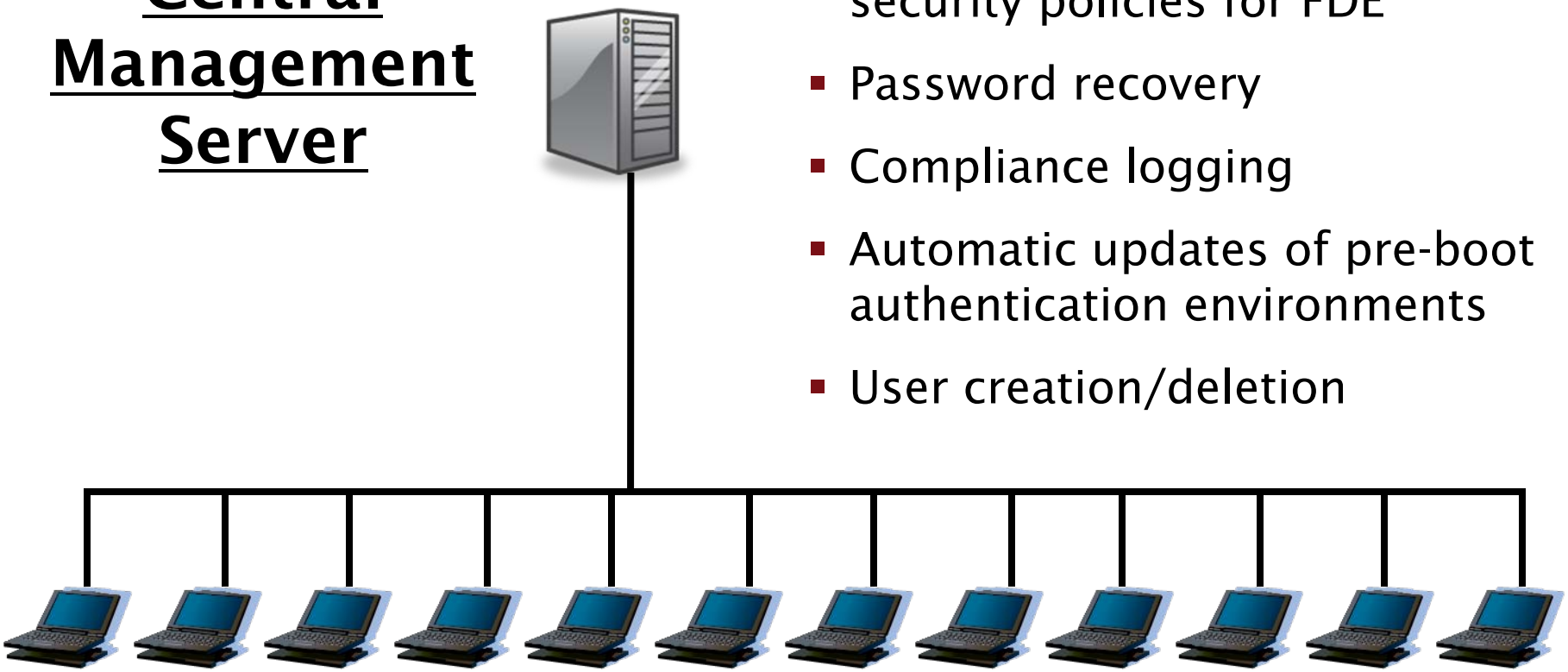


- Once Authenticated, the SED will act like a normal drive and the encryption is completely transparent to the OS, Applications, and User
- The solution is OS independent

TRUSTED COMPUTING GROUP™
Copyright© 2010 Trusted Computing Group.

Opal SEDs in Enterprise IT

Central Management Server



- Zero-touch configuration
- Central management of IT security policies for FDE
- Password recovery
- Compliance logging
- Automatic updates of pre-boot authentication environments
- User creation/deletion

TRUSTED COMPUTING GROUP™

Copyright© 2010 Trusted Computing Group.

Managing the SED

Before Unlocked, during Authentication

- Password recovery possible
- Remote unlock

After Unlocked, with O/S Present

- Change/reset Password or Required Credentials
- Add/remove/modify Users
- Add new partitions (or LBA ranges)
- Erase or re-provision partitions (or LBA ranges)
- Instant Secure Erase whole drive
- Revert to no management

Copyright© 2010 Trusted Computing Group.

What Keys are in the SED?

Data Encryption Key (DEK)

- The key used to encrypt all of the user data on the drive
- This key never leaves the drive
- This key is stored in an encrypted format somewhere in the Drive
- When the DEK is changed or erased, all existing data can not be decrypted

Authentication Key (AK)

- The key provided by the user to unlock the drive
- A hash of this key may be stored on the drive
- Once confirmed, this key is used to decrypt the DEK

Copyright© 2010 Trusted Computing Group.

Additional SED Basics

Power States

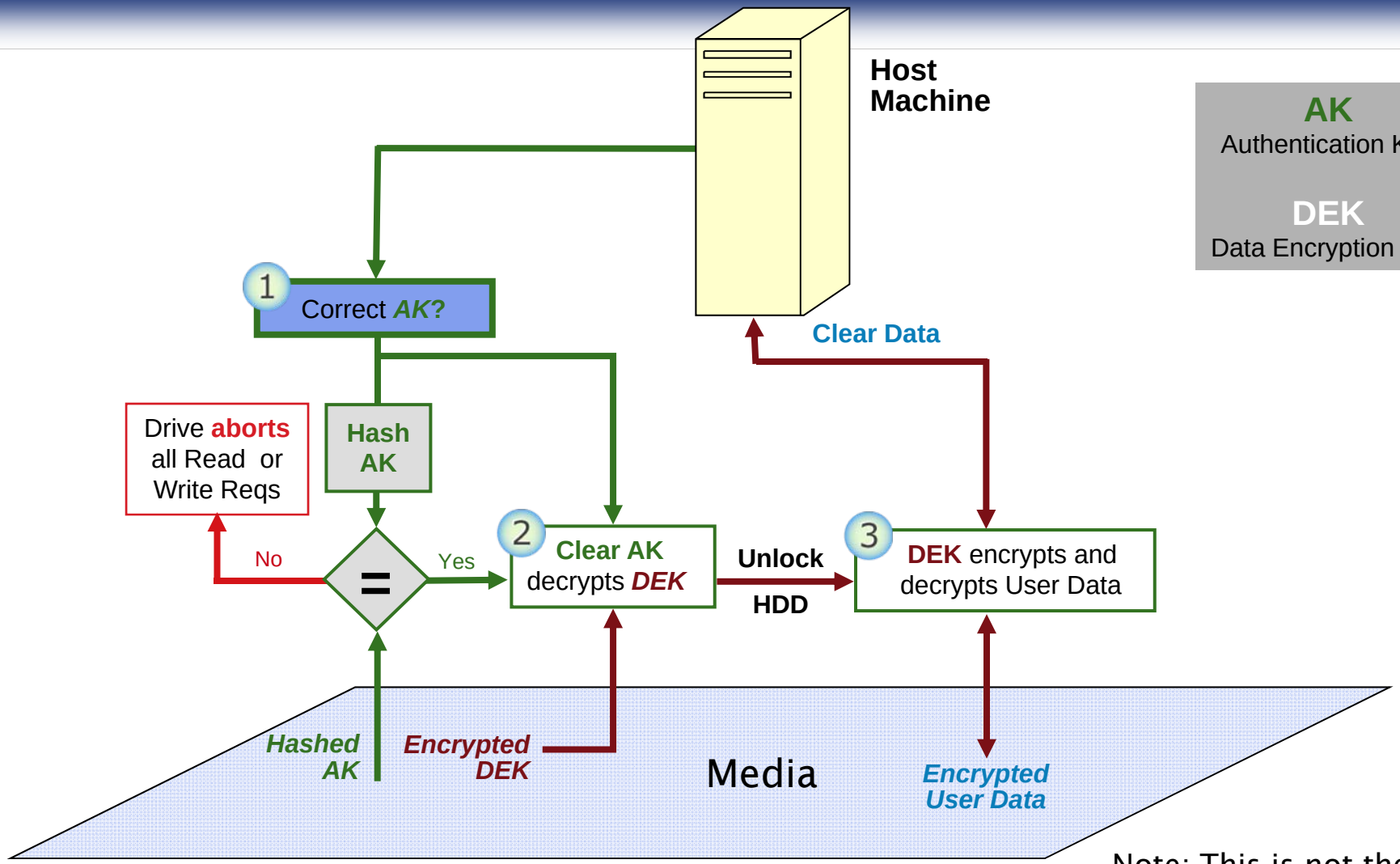
- When the SED is off, the Data Encryption Keys are encrypted and the data is cryptographically locked
- When the SED is powered on, the Authentication Key is required to “unlock” the Data Encryption Keys
- When the SED is powered off, the clear versions of the keys are gone

Ranges, Bands, or Regions

- The SED can be separated in Ranges, defined by LBAs
- Allows for Cryptographic Erase of a Range or whole drive
- Allows for different Authentication required for some Ranges

Copyright© 2010 Trusted Computing Group.

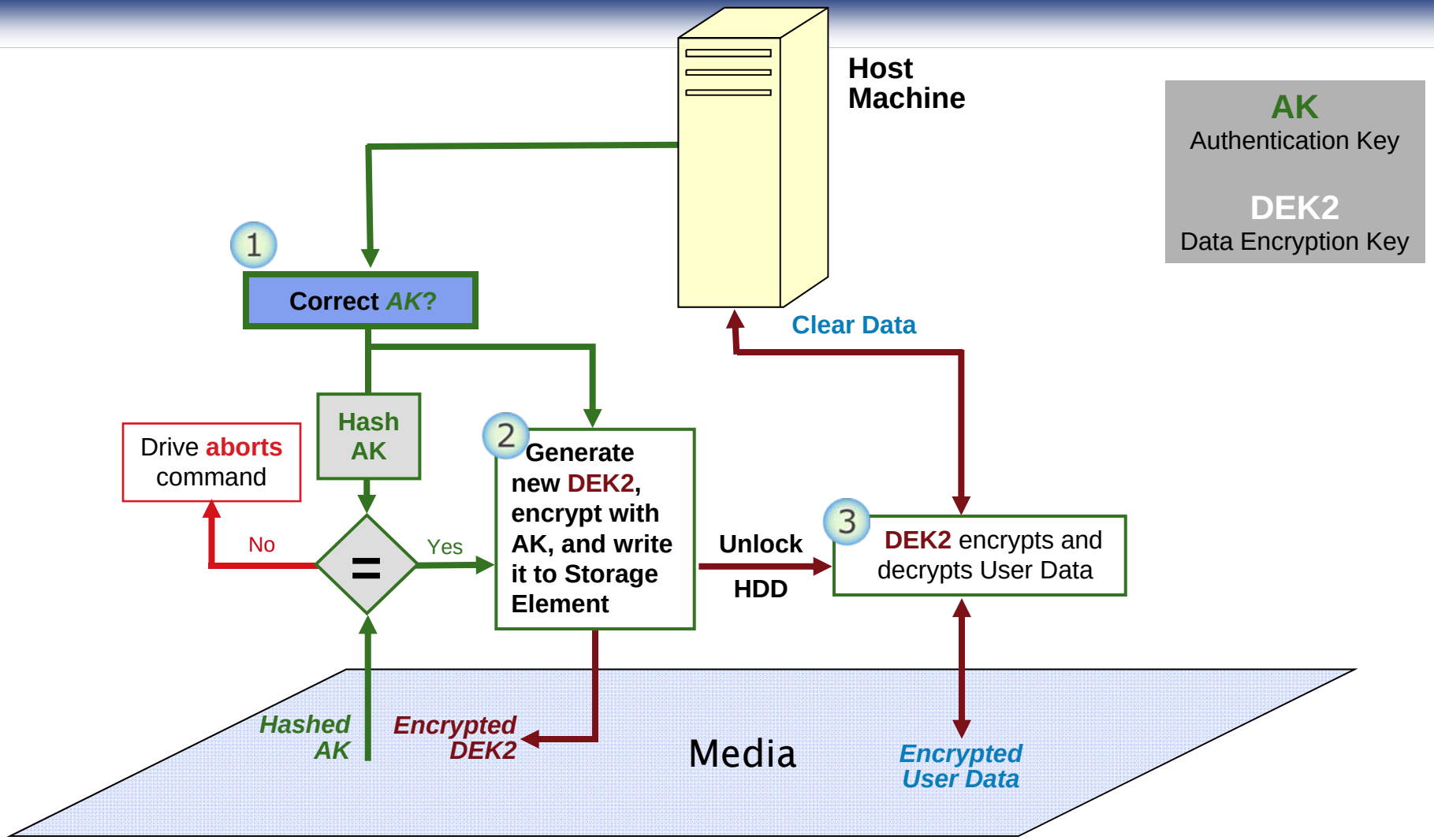
Keys and Unlocking



Note: This is not the only way to handle keys in a SED

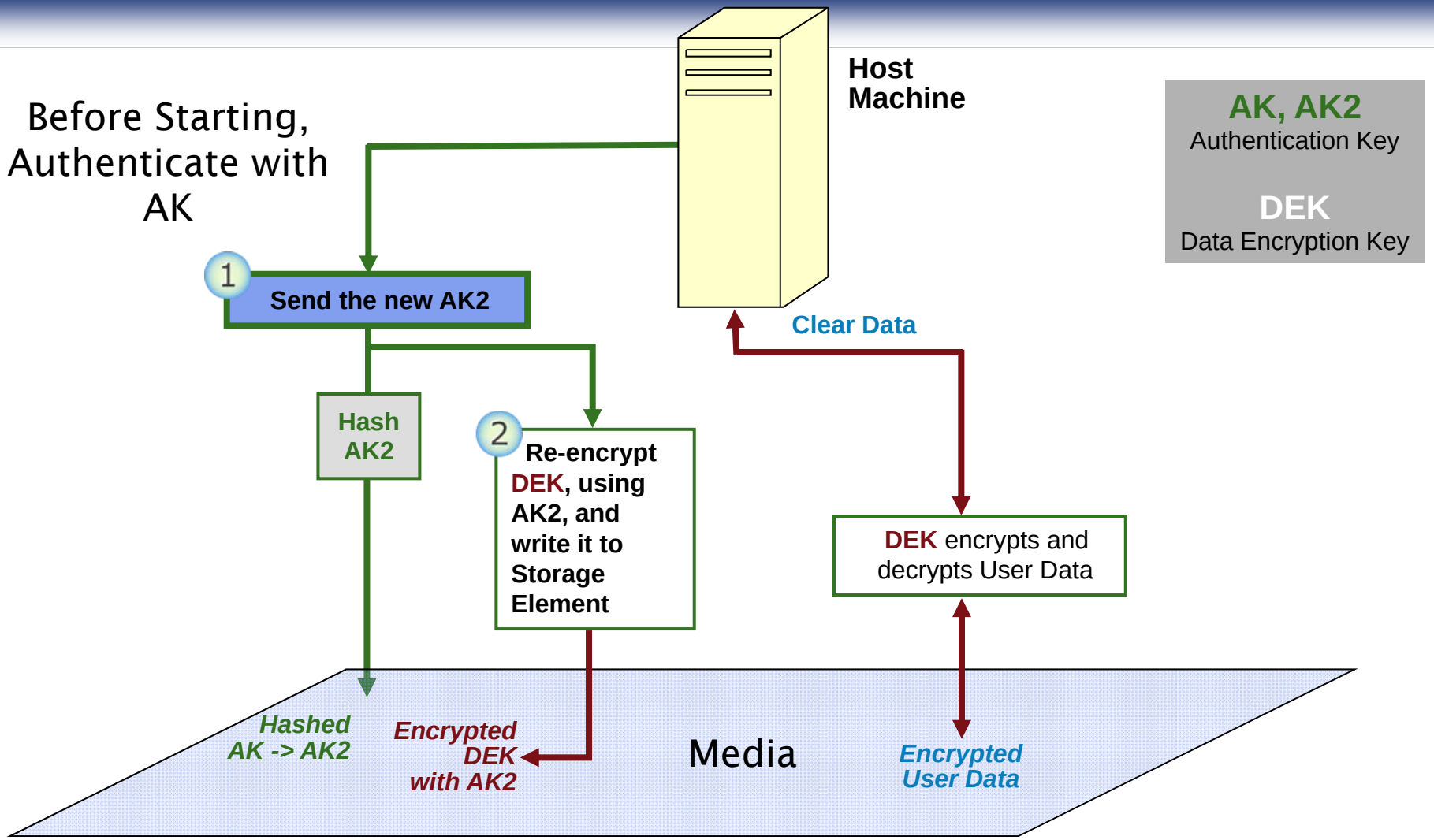
Copyright© 2010 Trusted Computing Group.

Erasing the SED or a Range in the SED



Copyright© 2010 Trusted Computing Group.

Changing the AK



Copyright© 2010 Trusted Computing Group.

Opal Self-Encrypting Drive (SED) Solution





- **SED Support:**
  - Highest performance solution for encryption of data-at-rest
  - Instant security – no lengthy initial encryption setup
  - Security policy enforcement – SED enforces policy set by administrator
  - Instant data sanitization – shred data in seconds, or even milliseconds, instead of hours of overwriting
- **Software Vendor Support:**
  - Complete, managed FDE solution from leading security software vendors
  - Feature-rich pre-OS authentication
  - Same look-and-feel as software-based FDE for heterogeneous environments

Copyright© 2010 Trusted Computing Group.

The Future: Self-Encrypting Drives

Encryption everywhere

- Data center/branch office to the USB drive

Standards-based

- Multiple vendors; interoperability

Unified key management

- Authentication key management handles all forms of storage

Simplified key management

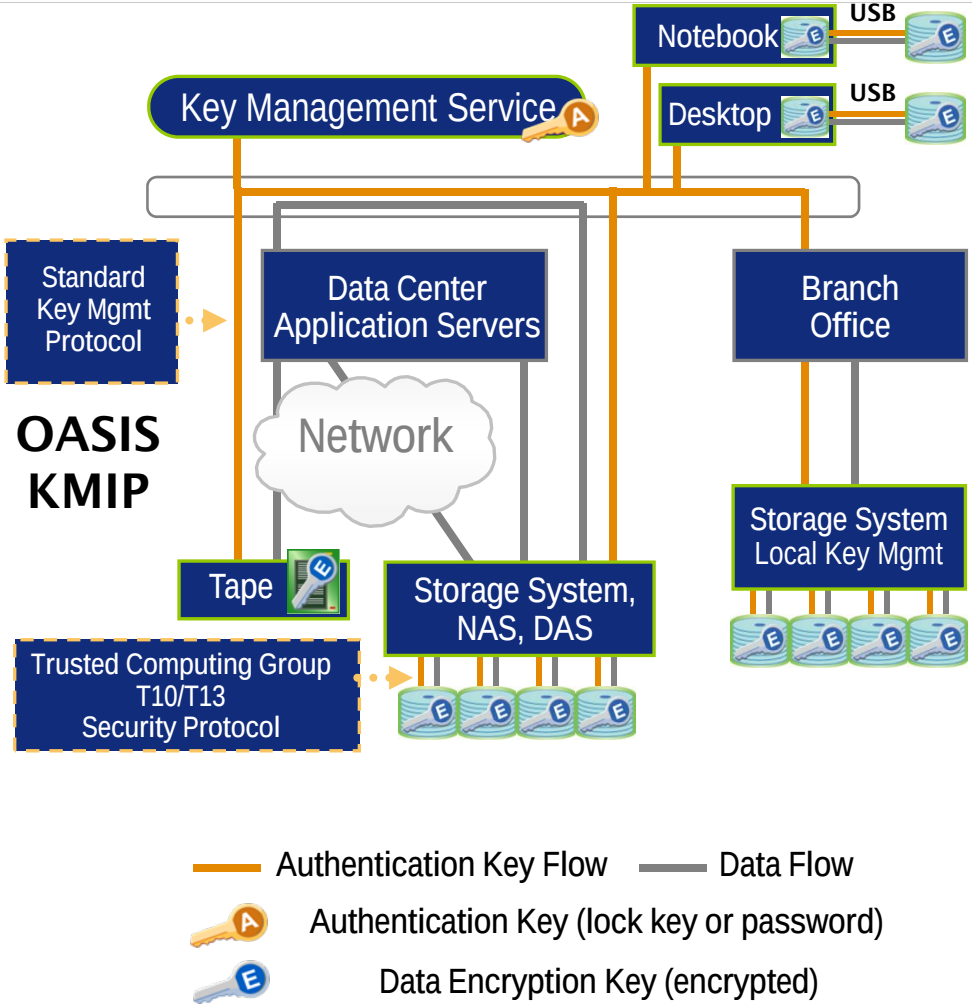
- Encryption keys never leave the drive. No need to track or manage

Transparent

- Transparent to OS, applications, application developers, databases, database administrators

Automatic performance scaling

- Granular data classification not needed



Copyright© 2010 Trusted Computing Group.

Resources

Live version of Webinar

http://www.trustedcomputinggroup.org/resources/where_is_your_data_tonight_a_lesson_in_avoiding_headlines_fines_or_worse

Commonly Asked Questions

http://www.trustedcomputinggroup.org/resources/commonly_asked_questions_and_answers_on_selfencrypting_drives

Additional Information:

http://www.trustedcomputinggroup.org/solutions/data_protection

http://www.trustedcomputinggroup.org/developers/storage