Solid–State Drives with Self–Encryption: Solidly Secure

Dr. Michael Willett

Storage Security Strategist

Text

SAMSUNG

Flash Memory Summit 2011
Santa Clara, CA

NOTE: Selected charts courtesy of TCG and SNIA

Monday, August 15, 2011

SOLID STATE DRIVES

10 Benefits For A Better Work Life

1. Fast Boot-up
2. Outlook File Search & Copy
3. Copying Files
4. Fast Application Start Up
5. Program Compilation
6. Virus Scan
7. Low Power Consumption
8. Multi-tasking
9. Video File Editing
10. Shock & Vibration Resistance

For a Better Work Life

SSD can save up to 61% of your work hour.

	HDD	SSD
Boot up	44s	29s
Outlook File Search	1m22s	9.5s
Outlook File Copy	39m22s	6m38s
Copying Files	21m15s	8m10s
Photoshop Start Up	55s	21.1s
PowerPoint Start Up	5s	0.4s
Multi-tasking	25m	9m50s
Video File Editing	14m16s	8m56s
Virus Scan	11m35s	6m4s
Program Compilation	1h25m	37m

4 hour

3h 19m 34s

61% time saving

1h 17m 38s

HDD

SSD

3

2

1

Test Environment : Windows Vista, Intel Core2Duo 2.4GHz, 2GB DDR2, ICH9M-E

Solid-State Drives

Monday, August 15, 2011

SOLID STATE DRIVES

Flash Memory SUMMIT

SSD ADVANTAGES

Reduced maintenance time and costs[1] → Save $$ on IT cost (TCO)

+

35% better performance[2] → Faster booting and application launching
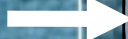
+

9 times more shock resistance[3] → Shock proof

+

67% more reliability (MTBF)[4] → Fewer drive crashes
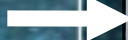
+

80% less power consumption[5] → Energy efficient and Green
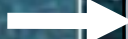
=

Right Solution

1) IDC white paper, Nov. 2007   2) SysMark 2007 Benchmark
3) 1500 G/0.5 ms SSD vs. 170 G/0.5 ms HDD
4) Reliability Demonstration Tests   5) 0.4 watts SSD vs. 2.0 watts HDD

IDC Study: The Cost of Owning a PC

or

True cost of an IT asset = direct + indirect costs over the life span

Cost factors:

- Acquisition
- Deployment
- Performance
- Support and maintenance
- Retirement

Example savings: SSD-based notebook PC: **improved reliability** = 35%, or **$30 per user per year**, reduction in lost productivity. Improved reliability **reduces the annual IT labor costs** to evaluate, fix, and/or replace failed or improperly working disks. The cost savings over HDD-based PCs is estimated to be 80%, or **$16 per user per year**.

Cost savings result from:

- increased user productivity
- higher reliability
- reduction of costs associated with support
- maintenance and retirement
- power savings

adding all of these cost benefits together....

http://www.samsung.com/global/business/semiconductor/products/flash/ssd/2008/down/

Monday, August 15, 2011

IDC Study: The Cost of Owning a PC

or

True cost of an IT asset = direct + indirect costs over the life span

Cost factors:

- • **Acquisition**
- • **Deployment**
- • **Performance**
- • **Support and maintenance**
- • **Retirement**

Example savings: SSD-based notebook PC: **improved reliability** = 35%, or **$30 per user per year**, reduction in lost productivity. Improved reliability **reduces the annual IT labor costs** to evaluate, fix, and/or replace failed or improperly working disks. The cost savings over HDD-based PCs is estimated to be 80%, or **$16 per user per year**.

Cost savings result from:

- • **increased user productivity**
- • **higher reliability**
- • **reduction of costs associated with support**
- • **maintenance and retirement**
- • **power savings**

Annual cost reduction up to $176/user annually

adding all of these cost benefits together….

http://www.samsung.com/global/business/semiconductor/products/flash/ssd/2008/down/

Monday, August 15, 2011

WHY ENCRYPT STORED DATA?

Flash Memory
SUMMIT

The Problem…

Since 2005, over 345,124,400 records containing sensitive personal information have been involved in security breaches

Reported Data Breaches Since February 2005 to Now

Source: Privacy Rights

In 2008, the average cost of a data breach was $6.65 million per affected corporation ($202 per record)

$6.65 Million Per Incident

http://www.privacyrights.org/ar/ChronDataBreaches.htm
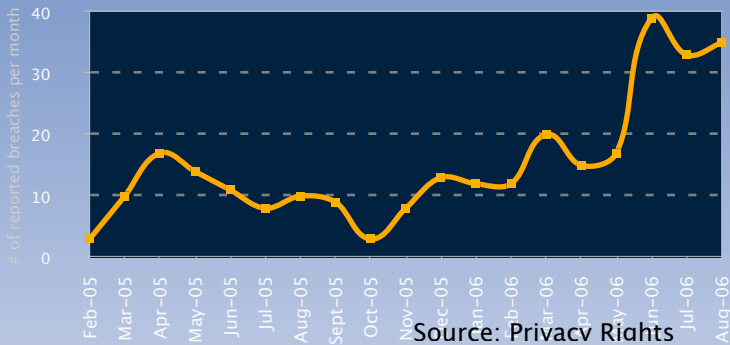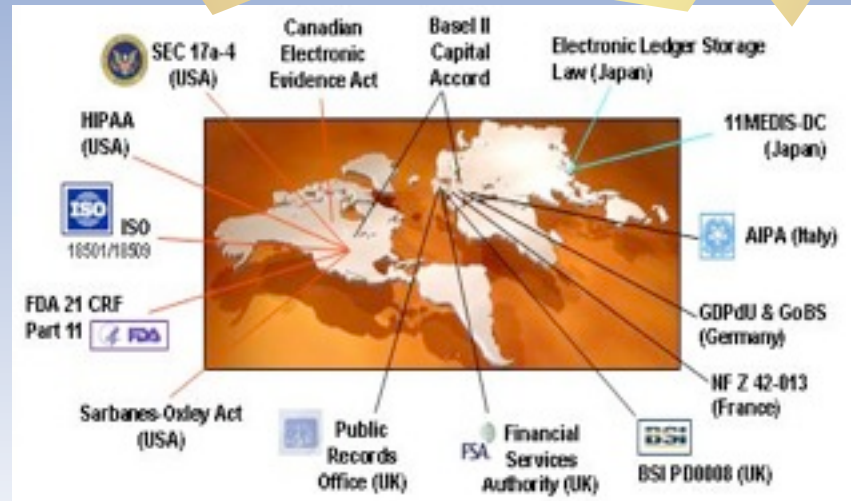
WHY ENCRYPT STORED DATA?

The Problem...

Since 2005, over 345,124,400 records containing sensitive personal information have been involved in security breaches.

In 2008, the average cost of a data breach was $6.65 million per affected corporation ($202 per Incident
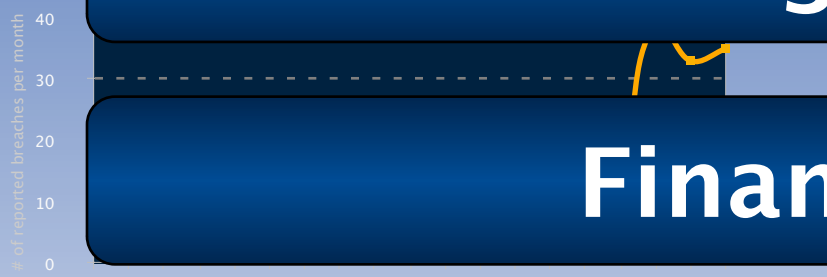
Legal

Financial

Reputation

http://www.privacyrights.org/ar/
ChronDataBreaches.htm

WHY ENCRYPT STORED DATA?

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

WHY ENCRYPT STORED DATA?

- Compliance
  - ➢ 45+ states have data privacy laws with encryption safe harbors
  - ➢ New federal 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

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

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

Self-Encrypting Drives (SED)

- 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

Trusted Storage Standardization

Trusted Storage Standardization

Published Storage Specifications

Authentication in the Drive

Storage Server

AK
Authentication Key
DEK
Data Encryption Key

Clear Data

1. Correct **AK?**

Drive responds to No Read or Write Reqs

Hash AK

Chip

No — = — Yes

2. **Clear AK** decrypts **DEK**

Unlock HDD/SSD

3. **DEK** encrypts and decrypts User Data

Hashed AK | **Encrypted DEK**

Encrypted User Data

Disc

Authentication in the Drive

Storage Server

AK
Authentication Key

DEK
Data Encryption Key

① Correct **AK**?

Clear Data

Chip

Drive responds to No Read or Write Reqs

Hash AK

No = Yes

② **Clear AK** decrypts **DEK**

Unlock HDD/SSD

③ **DEK** encrypts and decrypts User Data

Hashed AK

Encrypted DEK

Encrypted User Data

Disc

Cryptographic Erase

- **Description**
  - Cryptographic erase changes the drive encryption key
  - Data encrypted with previous key, unintelligible when **DEcrypted** with new key

- **Benefits**
  - Instantaneous "rapid" erase for secure disposal or re-purposing

Encryption Process

The quick brown fox jumps over the lazy dog

User Data

DEK

% $#@βδελιφρυιλ. σκδ% $#@ι&&6544τψ 899#@&$

Data on Drive

Change DEK Command

Decryption (After Erase)

☺☠✧☯☻☹⊕⌧ℳ
🔔☚②📜❀☾☪!
✂✳☽☎▭?&×※

Data After Erase

New DEK

% $#@βδελιφρυιλ. σκδ% $#@ι&&6544τψ 899#@&$

Data on Drive

No Performance Degradation

Encryption engine speed

Matches

Port's max speed

The encryption engine is in the controller ASIC

No Performance Degradation

Encryption engine speed

Matches

Port's max speed

The encryption engine is in the controller ASIC

Scales Linearly, Automatically

Network

Storage System

No Performance Degradation
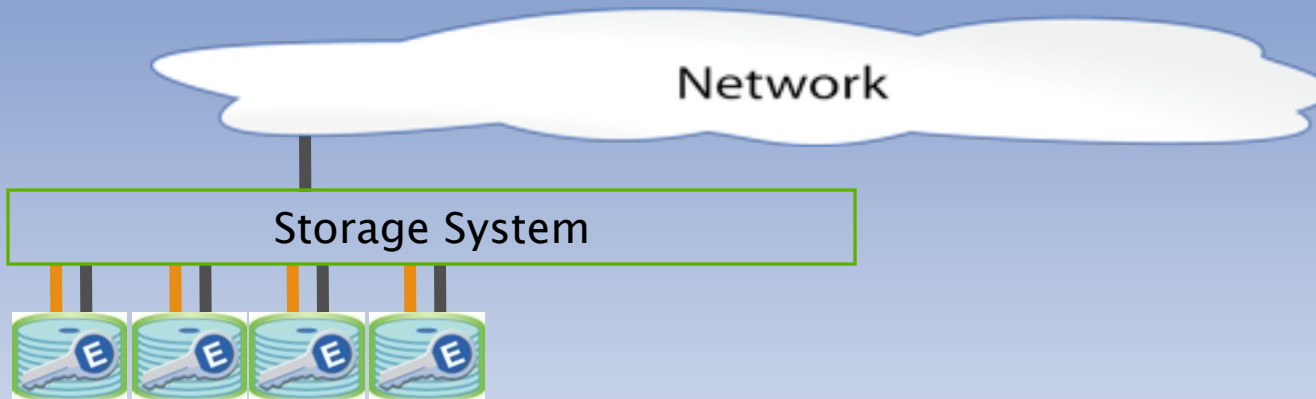
Encryption engine speed

Matches

Port's max speed

The encryption engine is in the controller ASIC

Scales Linearly, Automatically

Network

Storage System
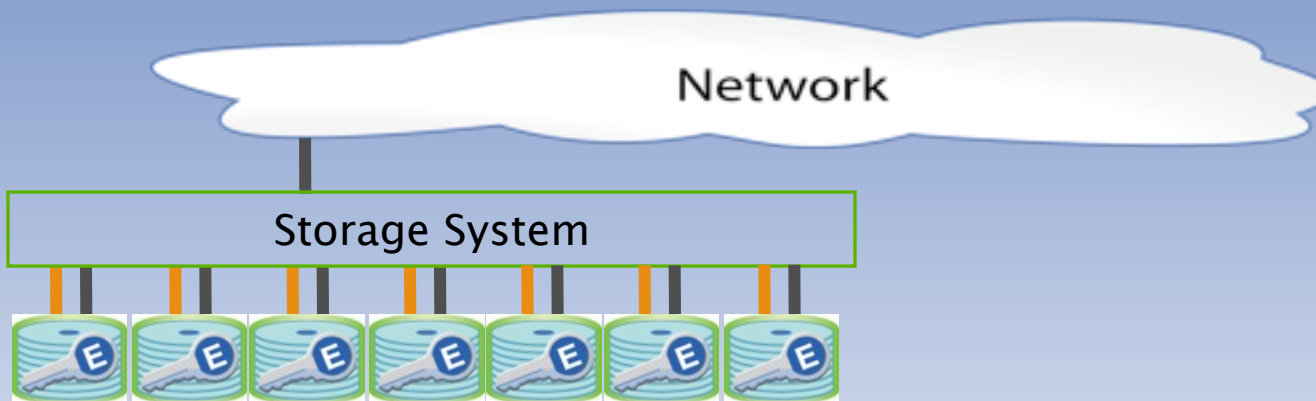
No Performance Degradation

Encryption engine speed

Matches

Port's max speed

The encryption engine is in the controller ASIC

Scales Linearly, Automatically

Network

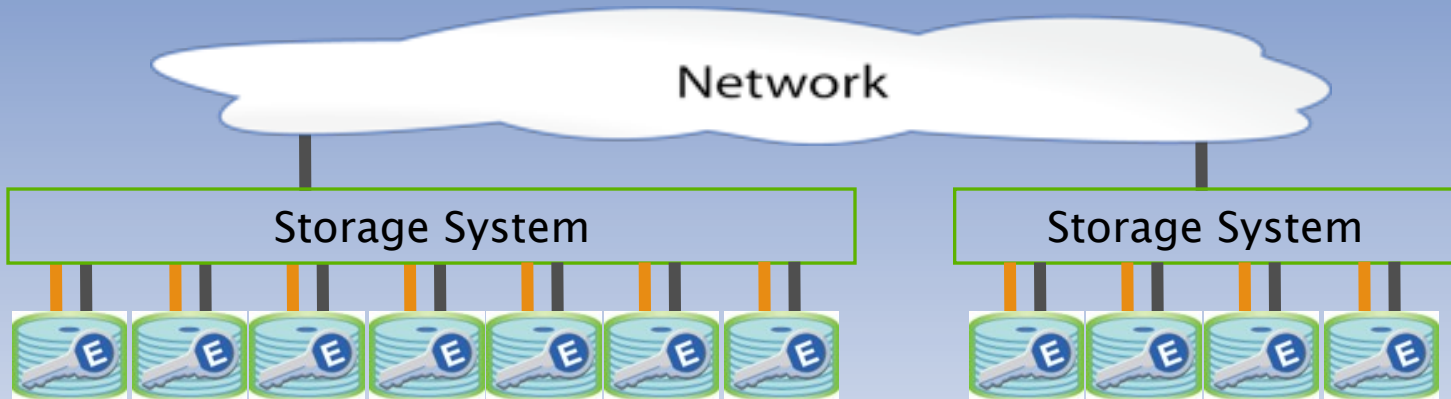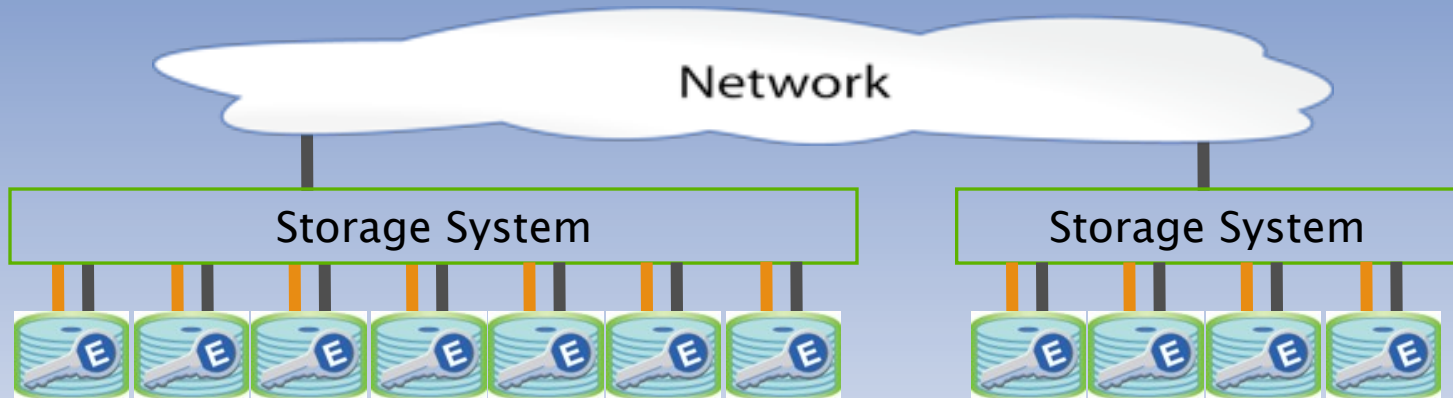Storage System

Storage System

No Performance Degradation

Encryption engine speed

Matches

Port's max speed

The encryption engine is in the controller ASIC

Scales Linearly, Automatically

Network

Storage System

Storage System

All data will be encrypted, with no performance degradation

How the Drive Retirement Process Works

Retirement Options

Retire Drive

- Replace
- Repair
- Repurpose

Remove ALL drives

Send even "dead" drives through

Queue in Secure Area

Transport Offsite

Queue in secure area

Overwriting takes days and there is no notification of completion from drive

Hard to ensure degauss strength matched drive type

Shredding is environmentally hazardous

Not always as secure as shredding, but more fun

S E C U R E ?

People make mistakes

"Because of the volume of information we handle and **the fact people are involved, we have occasionally made mistakes**." which lost a tape with 150,000 Social Security numbers stored at an Iron Mountain warehouse, October 2007[1]

IRON MOUNTAIN

99% of Shuttle Columbia's hard drive data recovered from crash site

Data recovery specialists at Kroll Ontrack Inc. retrieved 99% of the information stored on the charred Seagate hard drive's platters over a two day period.

– May 7, 2008 (Computerworld)

1. http://www.usatoday.com/tech/news/computersecurity/2008–01–18–penney–data–breach

How the Drive Retirement Process Works

Retirement Options

Retire Drive

- Replace
- Repair
- Repurpose

Drive Retirement is:

Expensive

Time-consuming

Error-prone

we have occasionally made ... mistakes.

which lost a tape with 150,000 Social Security numbers stored at an Iron Mountain warehouse, October 2007[1]

s hard drive data

Data recovery specialists at Kroll Ontrack Inc. retrieved 99% of the information stored on the charred Seagate hard drive's platters over a two day period.

– May 7, 2008 (Computerworld)

S E C U R E ?

1. http://www.usatoday.com/tech/news/computersecurity/2008-01-18-penney-data-breach_

Drive Retirement: Self-Encrypting Drives

Self-Encrypting Drives

S E C U R E

Retire Drive
- Replace
- Repair
- Repurpose

Remove ALL drives

Send even "dead" drives through

Queue in secure area

Transport Offsite

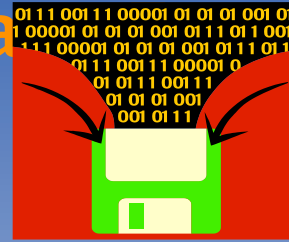Queue in secure area

Power Off = Locked and Encrypted = Secure

- Reduces IT operating expense
  - Eliminates the need to overwrite or destroy drive
  - Secures warranty and expired lease returns
  - Enables drives to be repurposed securely

- Provides safe harbor for most data privacy laws

16

Hardware-Based Self-Encryption versus Software Encryption

- **Transparency:** SEDs come from factory with encryption key already generated

- **Ease of management:** No encrypting key to manage

- **Life-cycle costs:** The cost of an SED is pro-rated into the initial drive cost; software has continuing life cycle 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

Hardware-Based Self-Encryption versus Software Encryption
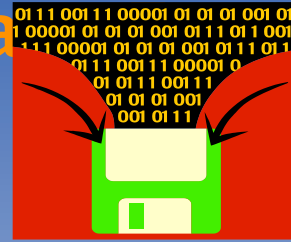
- **Transparency:** SEDs come from factory with encryption key already generated

- **Ease of management:** No encrypting key to manage

- **Life-cycle costs:** The cost of an SED is pro-rated into the initial drive cost; software has continuing life cycle 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)

Monday, August 15, 2011

Performance Comparisons: HDD and SSD, software versus SED

MB/Sec	HDD: no encryption	HDD: S/W encryption	HDD: SED	SSD: no encryption	SSD: S/W encryption	SDD: SED
Startup	7.90	6.97	7.99	82.50	47.90	95.33
App Loading	7.03	5.77	5.71	48.33	30.77	60.37
Modest size file test	6.13	5.00	5.28	41.13	26.77	50.40
Large Scale Data Read	84.67	52.88	82.75	178.00	70.23	169.33
Large Scale Data Write	79.60	49.50	50.31	170.80	63.60	164.50

http://www.trustedstrategies.com/

The Future: Self–Encrypting Drives

Encryption everywhere!
- Data center/branch office to the USB drive

Standards–based
- Multiple vendors; interoperability

Unified key management
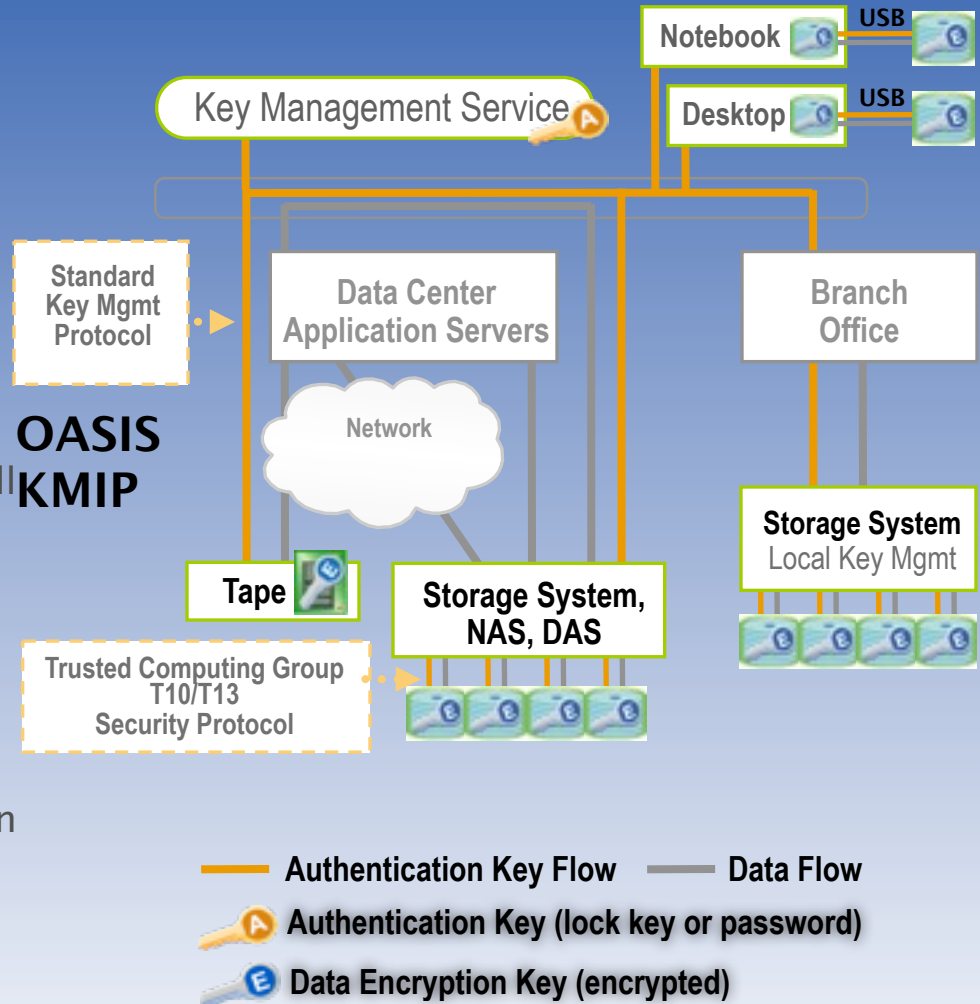- Authentication key management handles all forms of storage

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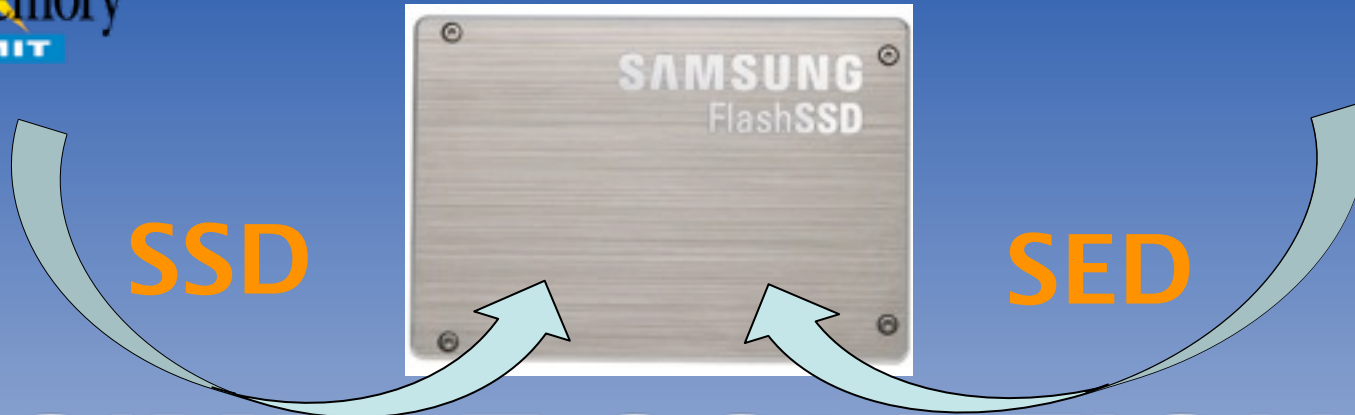- Encryption keys never leave the drive. No need to track or manage.

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

Automatic performance scaling
- Granular data classification not needed

Key Management Service

Notebook — USB

Desktop — USB

Standard Key Mgmt Protocol

Data Center Application Servers

Branch Office

OASIS KMIP

Network

Storage System
Local Key Mgmt

Tape

Storage System, NAS, DAS

Trusted Computing Group T10/T13 Security Protocol

Authentication Key Flow   Data Flow

Authentication Key (lock key or password)

Data Encryption Key (encrypted)

Solid-State Drive + Self-Encrypting

SSD

SED

SIMPLE SOLUTION

- Reduced TCO
- Increased productivity
- Better Performance
- More shock resistance
- Better reliability
- Less power use
- Cost reduction up to $176
  (per user, annually)

- Simplified Management
- Robust Security
- Compliance "Safe Harbor"
- Cut Disposal Costs

- Scalable
- Interoperable
- Integrated
- Transparent