SNIA™
Global Education

# Implementing Stored-Data Encryption

**Dr. Michael Willett**
**VP Marketing**
**Drive Trust Alliance**

# SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

# Abstract

SNIA
Global Education

# Implementing Stored-Data Encryption

Data security is top of mind for most businesses trying to respond to the constant barrage of news highlighting data theft, security breaches, and the resulting punitive costs.  Combined with litigation risks, compliance issues and pending legislation, companies face a myriad of technologies and products that all claim to protect data-at-rest on storage devices. What is the right approach to encrypting stored data?

The Trusted Computing Group, with the active participation of the drive industry, has standardized on the technology for self-encrypting drives (SED): the encryption is implemented directly in the drive hardware and electronics. Mature SED products are now available from all the major drive companies, both HDD (rotating media) and SSD (solid state) and both laptops and data center. SEDs provide a low-cost, transparent, performance-optimized solution for stored-data encryption. SEDs do not protect data in transit, upstream of the storage system.

For overall data protection, a layered encryption approach is advised. Sensitive data (eg, as identified by specific regulations: HIPAA, PCI DSS) may require encryption outside and upstream from storage, such as in selected applications or associated with database manipulations.

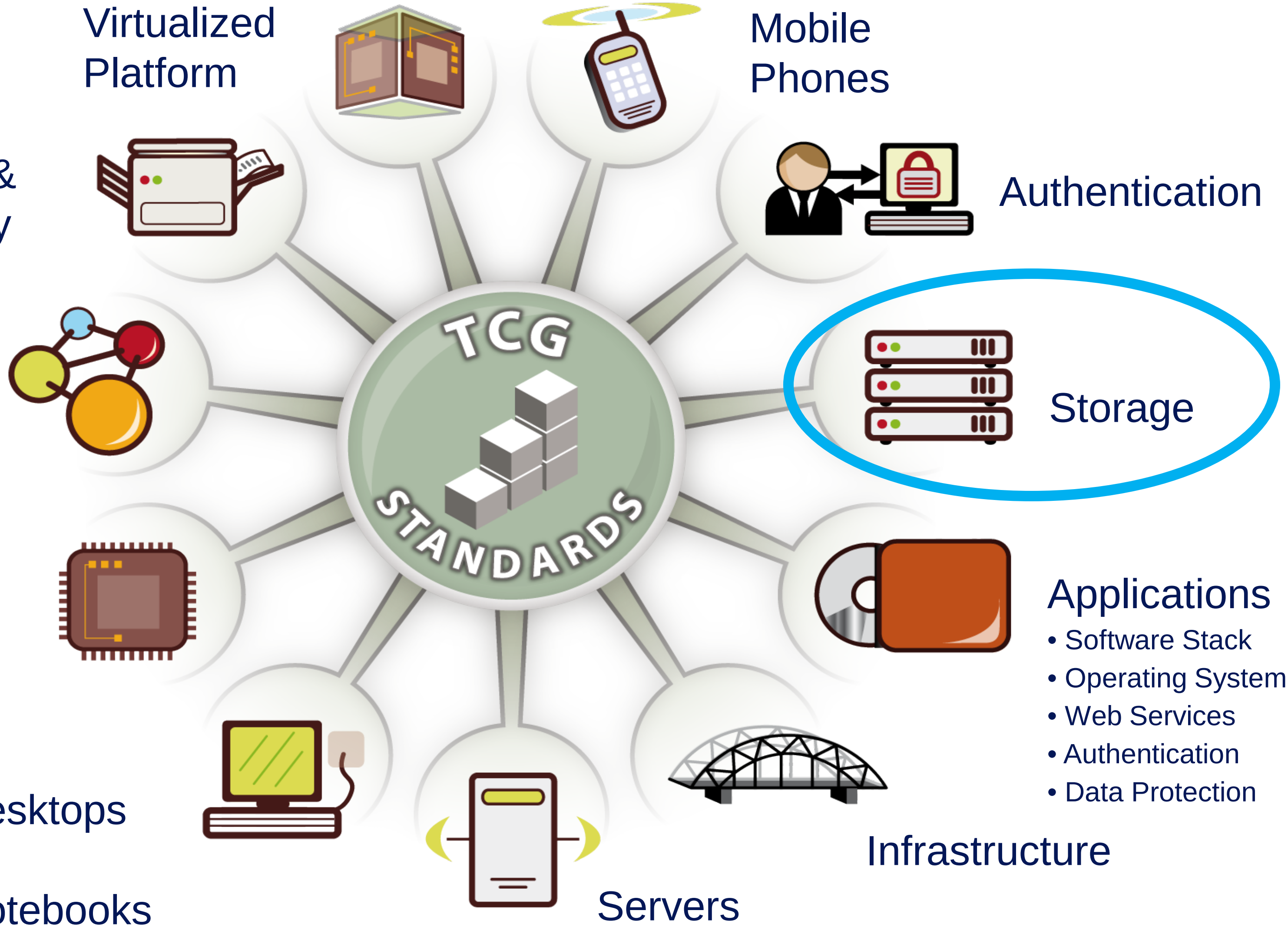
This tutorial will examine a ‘pyramid’ approach to encryption: selected, sensitive data encrypted at the higher logical levels, with full data encryption for all stored data provided by SEDs. The attendee should learn:

The mechanics of SEDs, as well as application and database-level encryption

The pros and cons of each encryption subsystem

The overall design of a layered encryption approach

# Trusted Computing Group Standards



Virtualized Platform

Mobile Phones

Printers & Hardcopy

Authentication

Network Security

Storage

Security Hardware

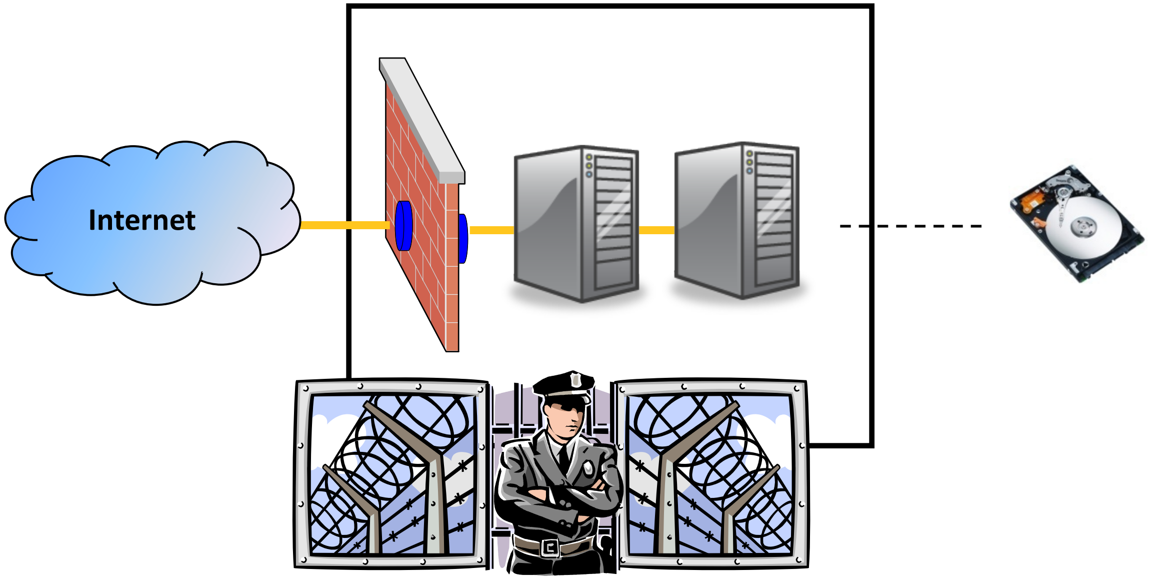
Applications
- Software Stack
- Operating Systems
- Web Services
- Authentication
- Data Protection

Desktops & Notebooks

Servers

Infrastructure

# IT Security Today



- Corporations spend millions to protect their networks, devices & data…
  - **Physical security, firewalls, intrusion detection, etc…**

- …But don't always understand the risk posed by internal misplacement, re-purposing, and disposal processes.

**Front Door**

**Back Door!!**

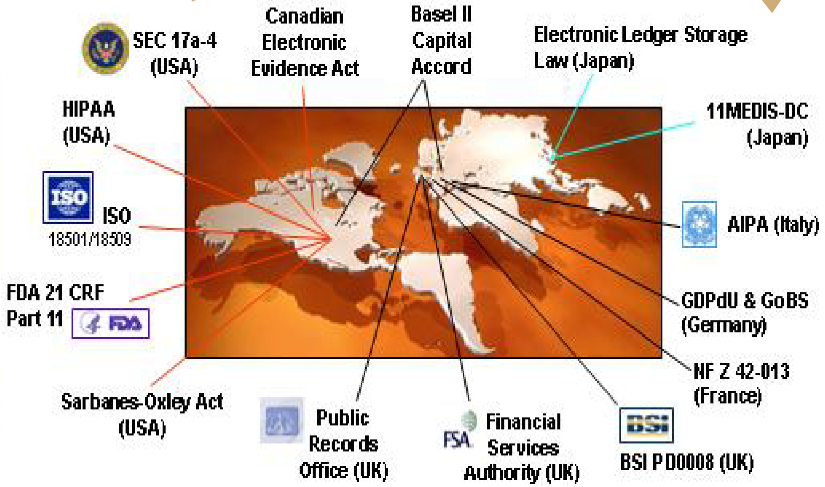
# Use Case : Stored Data Protection

# The Problem…

**2005-2013: over 864,108,052 records containing sensitive personal information have been involved in security breaches**

**In 2013, U.S. businesses paid an average cost of $5.4 million per data breach; that's $188 per record**

**$5.4 Million Per Incident**



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

http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-2013

# The Problem…

**2005-2013: over 864,108,052 records containing sensiti… involve…**

**Legal**

**…age cost of $5.4 …er record**

**$5.4 Million Per Incident**

**Financial**

**Reputation**

…torage
11MEDIS-DC (Japan)
…(USA)
AIPA (Italy)
DPdU & GoBS (Germany)
NF Z 42-013 (France)
Sarbanes-Oxley Act (USA)
Public Records Office (UK)
FSA
Financial Services Authority (UK)
BSI
BSI PD0008 (UK)

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

http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-2013

# Breach Notification Legislation

## Example: California

**“… any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person…”**

Encryption “safe harbor”

# Why Encrypt Data-At-Rest?

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

- Compliance
  - **48+ U.S. states have data privacy laws with encryption "safe harbors", which exempt encrypted data from breach notification**[1]

- EU: Data Protection Directive 95/46/EC (27 countries) replaced with
- European Data Protection Regulation [4] : **requires breach notification** [3]

- Exposure of data loss is expensive ($6.65 Million on average per incident[2])
- Obsolete, Failed, Stolen, Misplaced…
  - **Nearly ALL drives leave the security of the data center**
  - **The vast majority of retired drives are still readable**

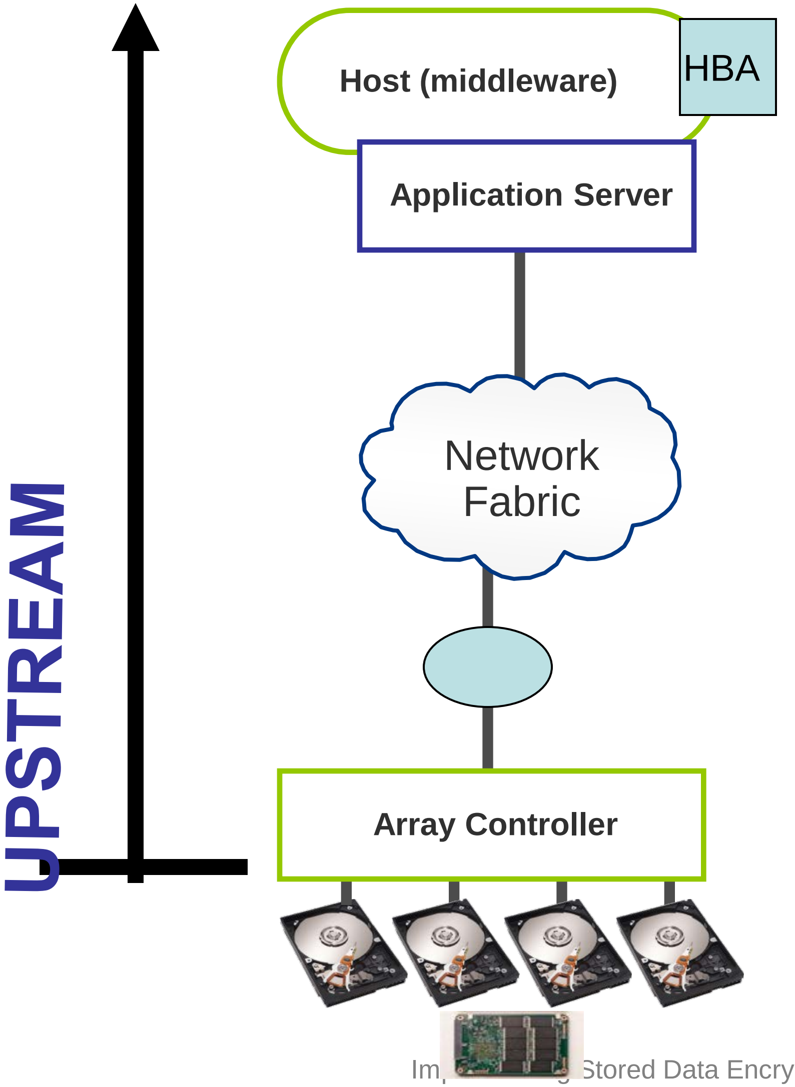
[1] http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx

[2] Ponemon Institute, Annual US Cost of Data Breach Study – www.ponemon.org

[3] https://www.eiseverywhere.com/file_uploads/4982c29aa16310269434b49b0ac62eed_EricHibbard_Data-Breach-Encryption-Safe-Harbor_Final.pdf

[4] http://en.wikipedia.org/wiki/General_Data_Protection_Regulation

# Encryption can be done in a number of places…



Host middleware

Host HBA (h/w adapter)

Application

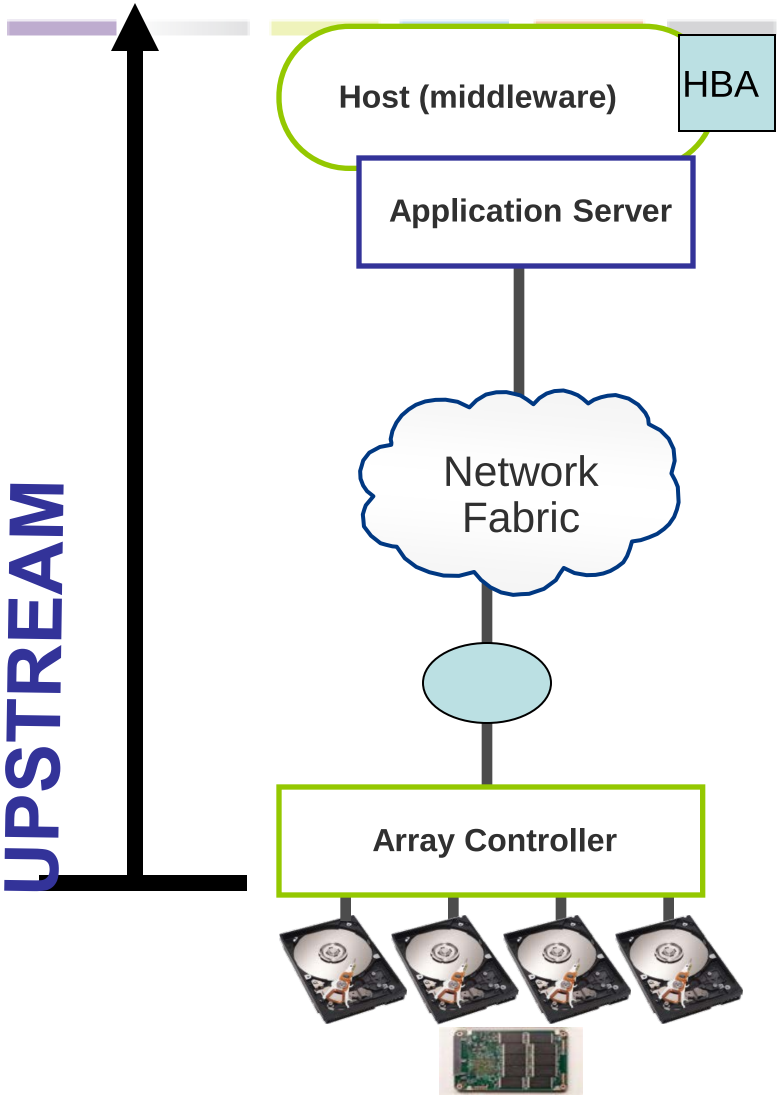
Switch

“Bump in the wire” appliance

Array controller

Drive (HDD, SSD)

# Encryption can be done in "layers"…



Host middleware

Host HBA (h/w adapter)

Application

Switch

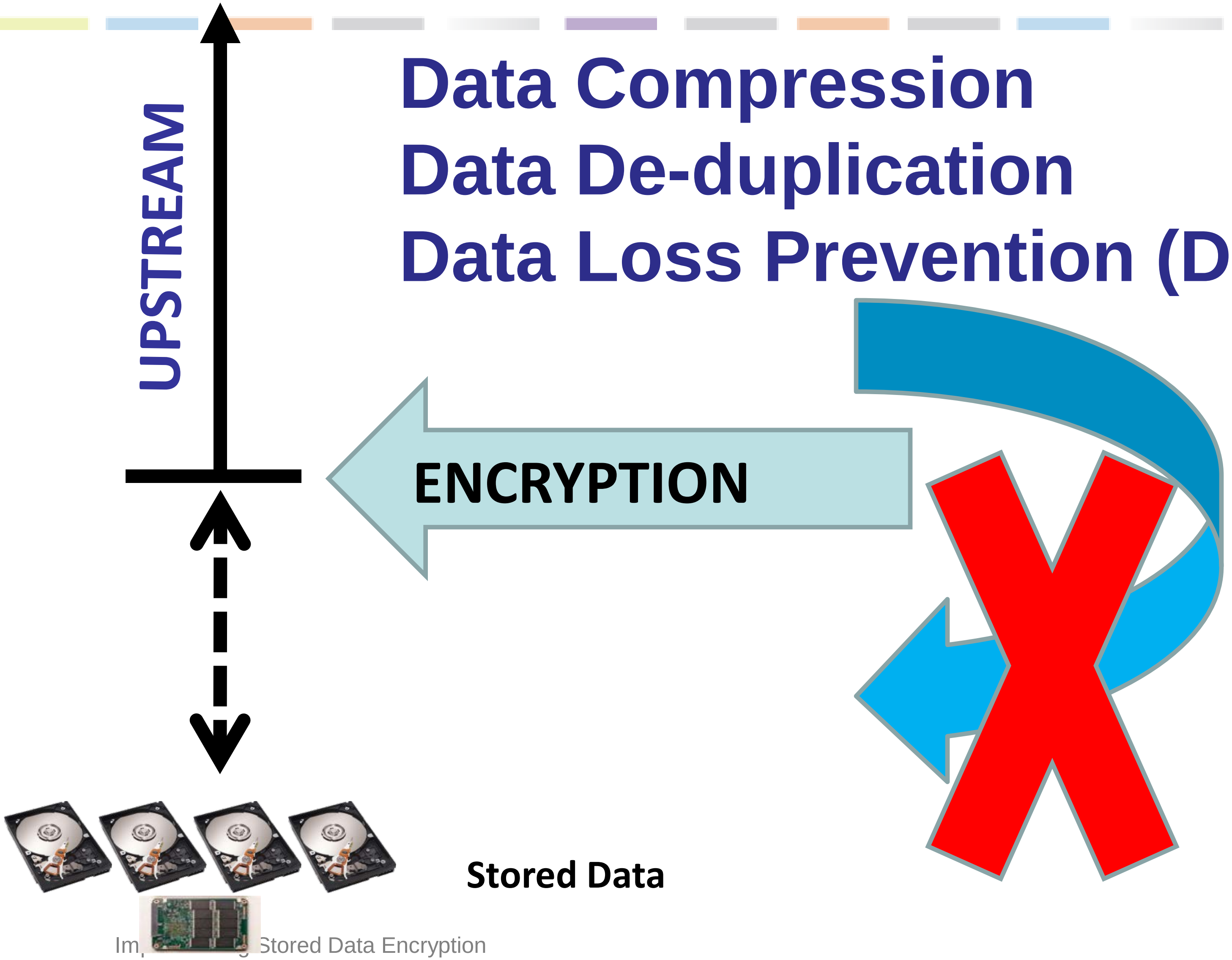
"Bump in the wire" appliance

Array controller

Drive (HDD, SSD)

**DIFFERENT THREAT SCENARIOS**

# Encryption upstream can affect other processes



Data Compression
Data De-duplication
Data Loss Prevention (DLP)

# Trusted Storage Standardization

TRUSTED COMPUTING GROUP™

Published Storage Specifications

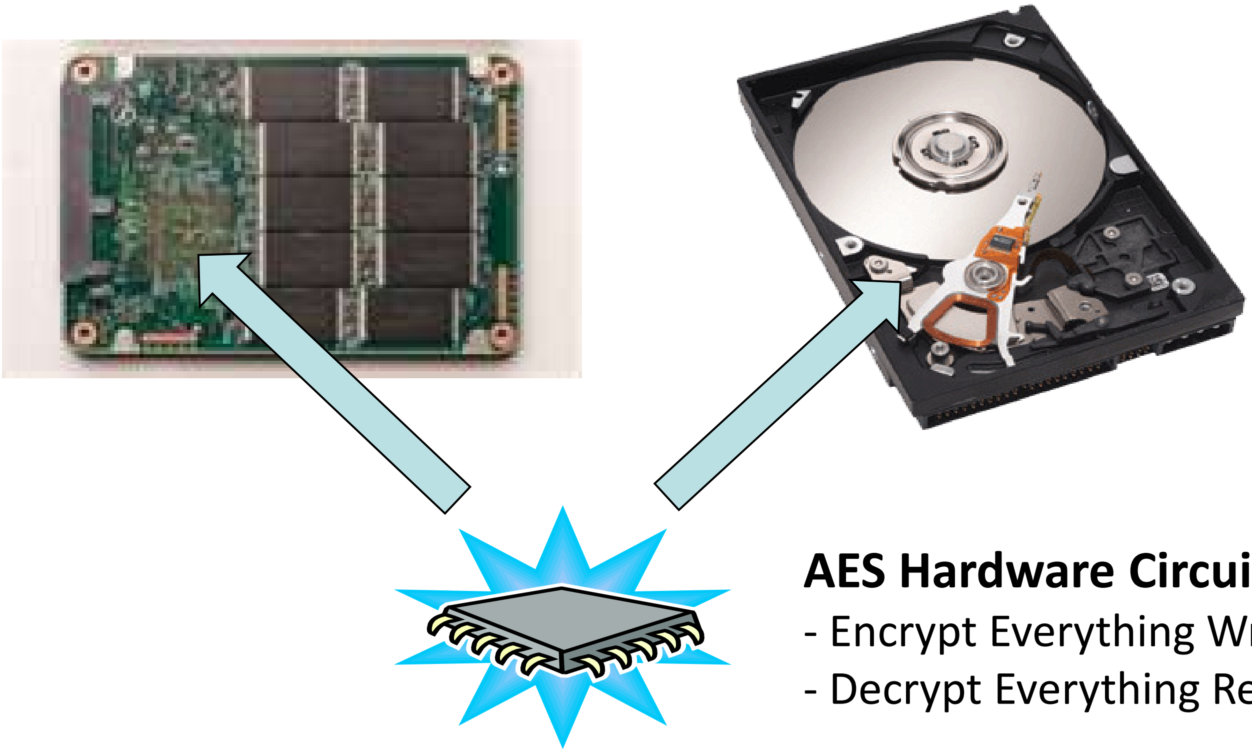
Self-Encrypting Drives (SED)

# What  is a Self-Encrypting Drive (SED)?

Trusted Computing Group

SED Management Interface

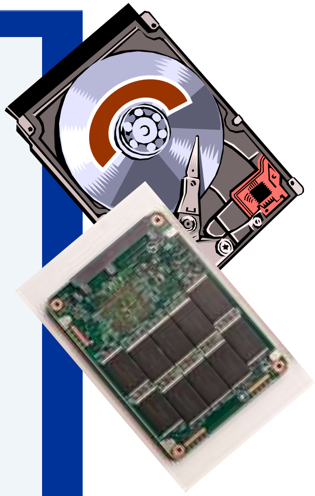
Interface



**AES Hardware Circuitry**

- Encrypt Everything Written
- Decrypt Everything Read

# Why Put Security Directly in Drive Storage?



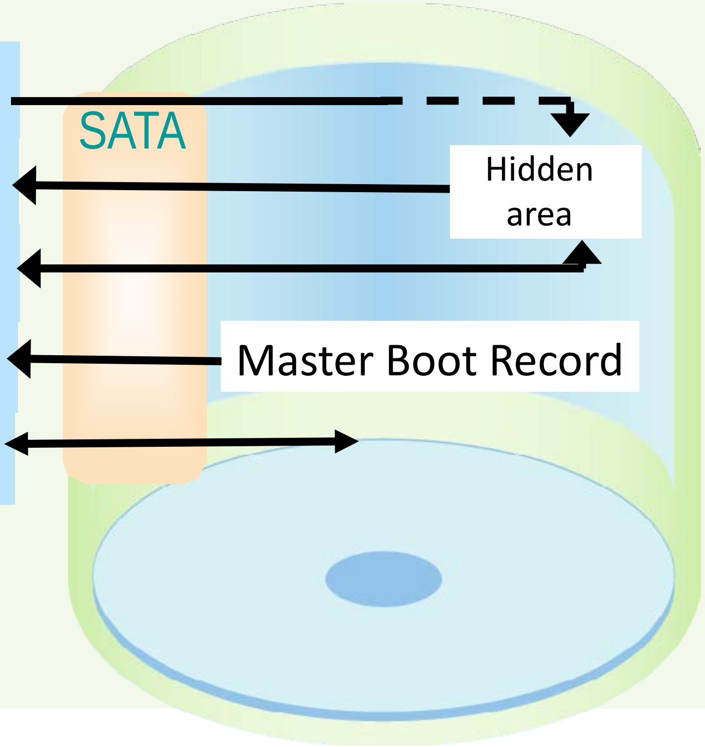
## 3 Simple reasons

- Storage for secrets with strong access control
  - Inaccessible using traditional storage access
  - Arbitrarily large memory space
  - Gated by access control
- Unobservable cryptographic processing of secrets
  - Processing unit “welded” to storage unit
  - “Closed”, controlled environment
- Custom logic for faster, more secure operations
  - Inexpensive implementation of modern cryptographic functions
  - Complex security operations are feasible

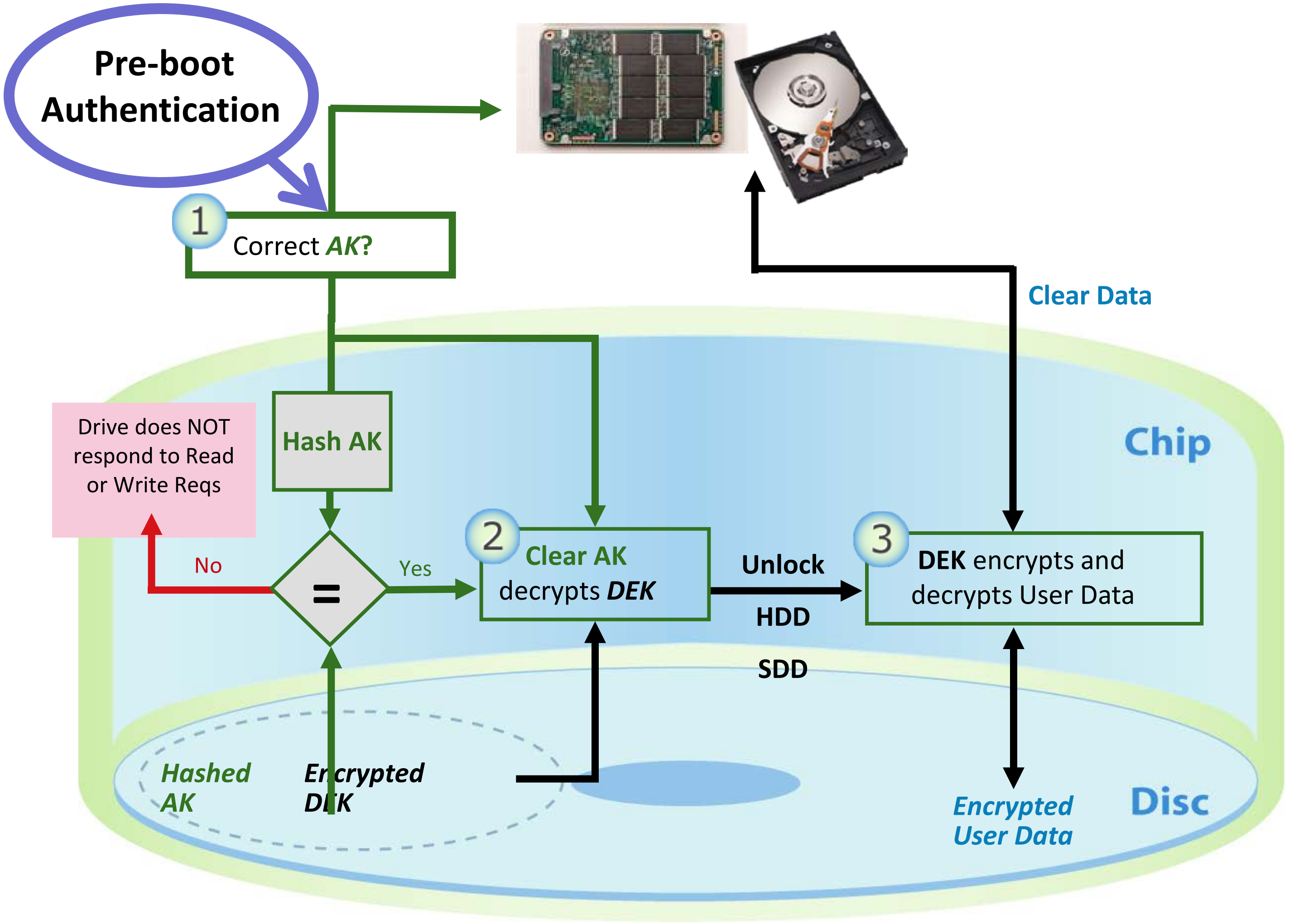
# Client Security: Pre-Boot Authentication

- **Transparency: Master boot record and OS are unmodified**
- **Protected from malicious software:  Authentication occurs before OS (and any malicious software) is loaded**
- **The master boot record can't be corrupted:  The entire drive, including the master boot record, is encrypted**

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



# Authentication in the Drive



**AK**
Authentication Key

**DEK**
Data Encryption Key

# Crypto Erase

SNIA™ Global Education

## Description

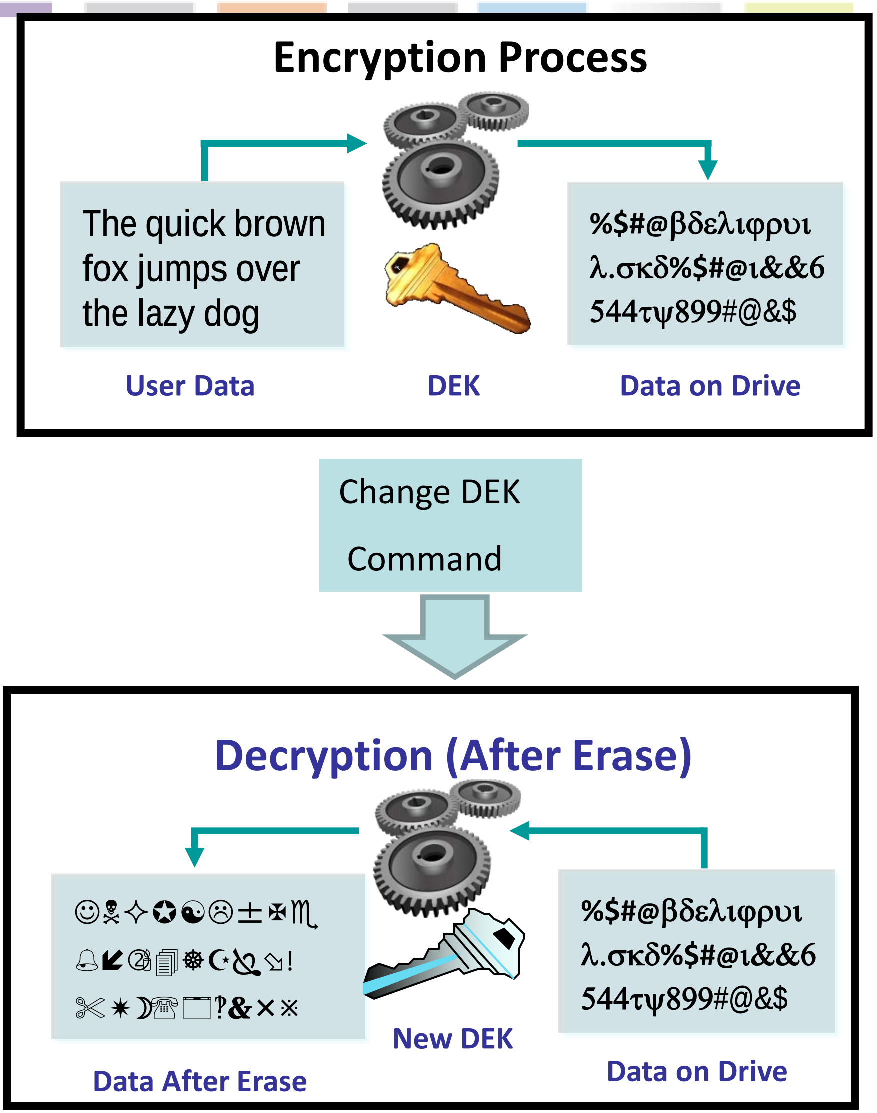
- Cryptographic erase changes the drive encryption key
- Data encrypted with previous key, unintelligible when **DEcrypted** with new key

## Benefits

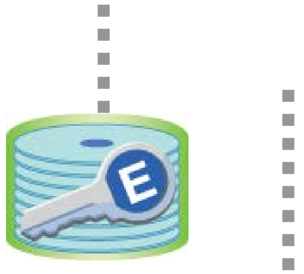
- Instantaneous “rapid” erase for secure disposal or re-purposing

- Revision 1 of U.S. NIST SP800-88: **Guidelines for Media Sanitization** under way to support Crypto Erase

http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf



# No Performance Degradation



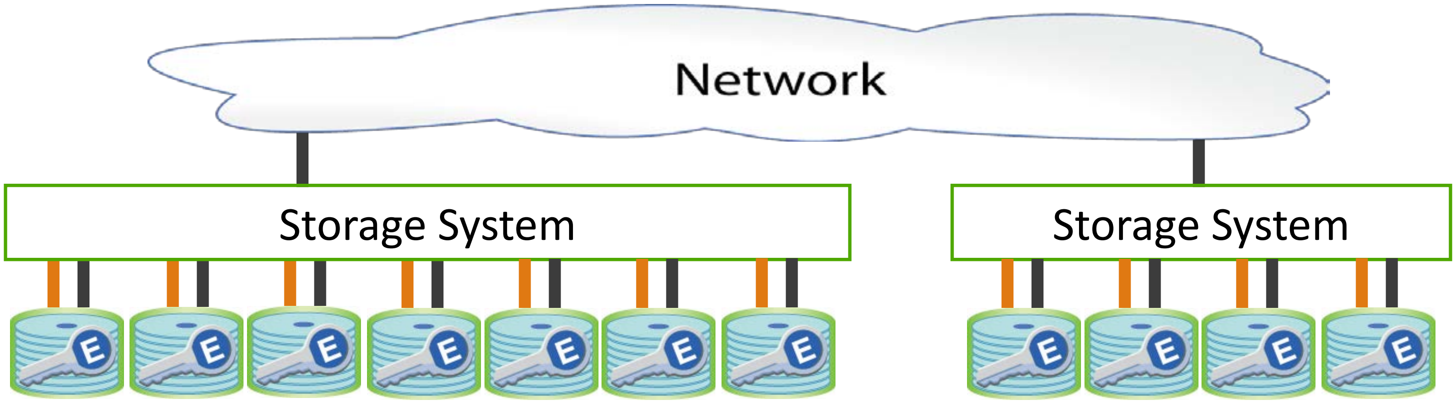
Encryption engine speed

**Matches**

Port’s max speed

**The encryption engine is in the drive electronics**

Scales Linearly, Automatically



All data will be encrypted, with no performance degradation

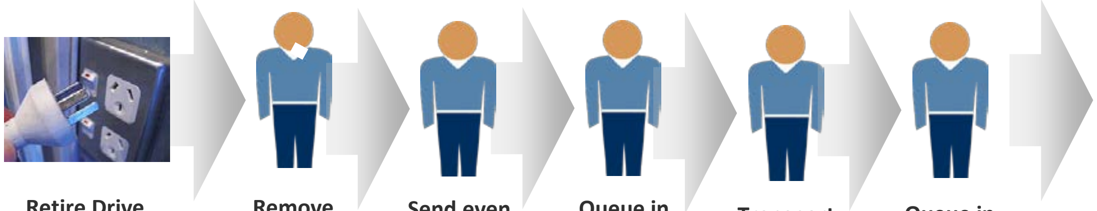
# IT Retires Drives Constantly

- All Drives are Eventually Retired
  - End of Life
  - Returned for Expired Lease
  - Returned for Repair / Warranty
  - Repurposed
- 50,000 drives leave data centers daily
- Exposure of data is expensive - $6.65 million on average
- 90% of retired drives are still readable (IBM study[1])

**Needed: A simple, efficient, secure way to make retired drive data unreadable**

[1] http://www.redbooks.ibm.com/redpapers/pdfs/redp4529.pdf

# How the Drive Retirement Process Works



- Replace
- Repair
- Repurpose

## Retirement Options

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**."

IRON MOUNTAIN

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

**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_

# Disposal Options Are Riddled with Shortcomings

## Formatting the drive or deleting the data

- *Doesn’t remove the data - data is still readable*

## Shredding

- *Very costly; time-consuming; dependent on technicians who have other duties*
- *Environmentally hazardous*
- *Loss of investment*

## Smashing the disk drive

- *Not always as secure as shredding, but more fun*
- *Environmentally hazardous*
- *Loss of investment*

## Over-writing

- *Takes hours-to-days*
- *Error-prone; no notification from the drive of overwrite completion*

## Degaussing the disk drive

- *Difficult to ensure degauss strength matched type of drive*
- *Very costly; error-prone; dependent on technicians who have other duties*
- *Loss of investment*

## Disposing via professional offsite services

- *Costly*
- *No guarantee of disposal*
- *Drive is exposed to the tape’s falling-off-the-truck issue*

# How the Drive Retirement Process Works

SNIA™ Global Education

## Retirement Options

Retire D

- Replace
- Repair
- Repurp

takes days
no
of
from drive

ure degauss
tched drive

s
tally

as secure
, but

S
E
C
U
R
E
?

# Drive Retirement is:

# *Expensive*

# *Time-consuming*

# *Error-prone*

we have occasionally made mistakes.

IRON MOUNTAIN

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

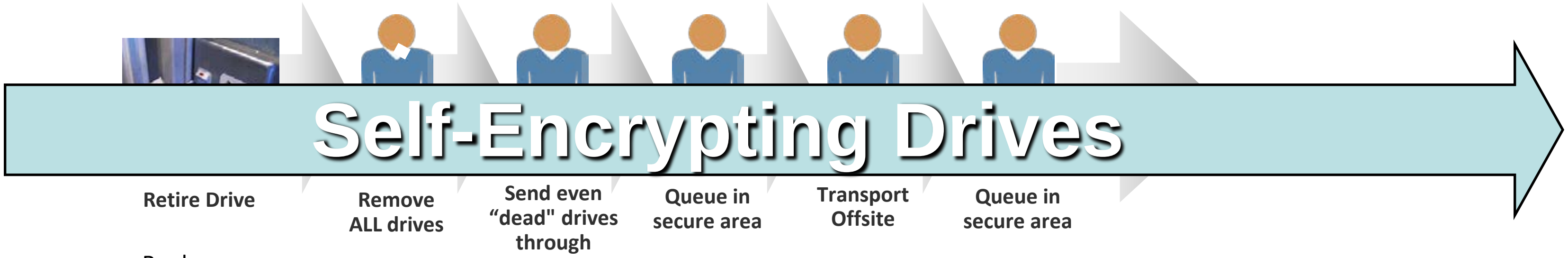
**99% of Shuttle Columbia's hard drive data recovered from crash site**

**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_

# Drive Retirement: Self-Encrypting Drives



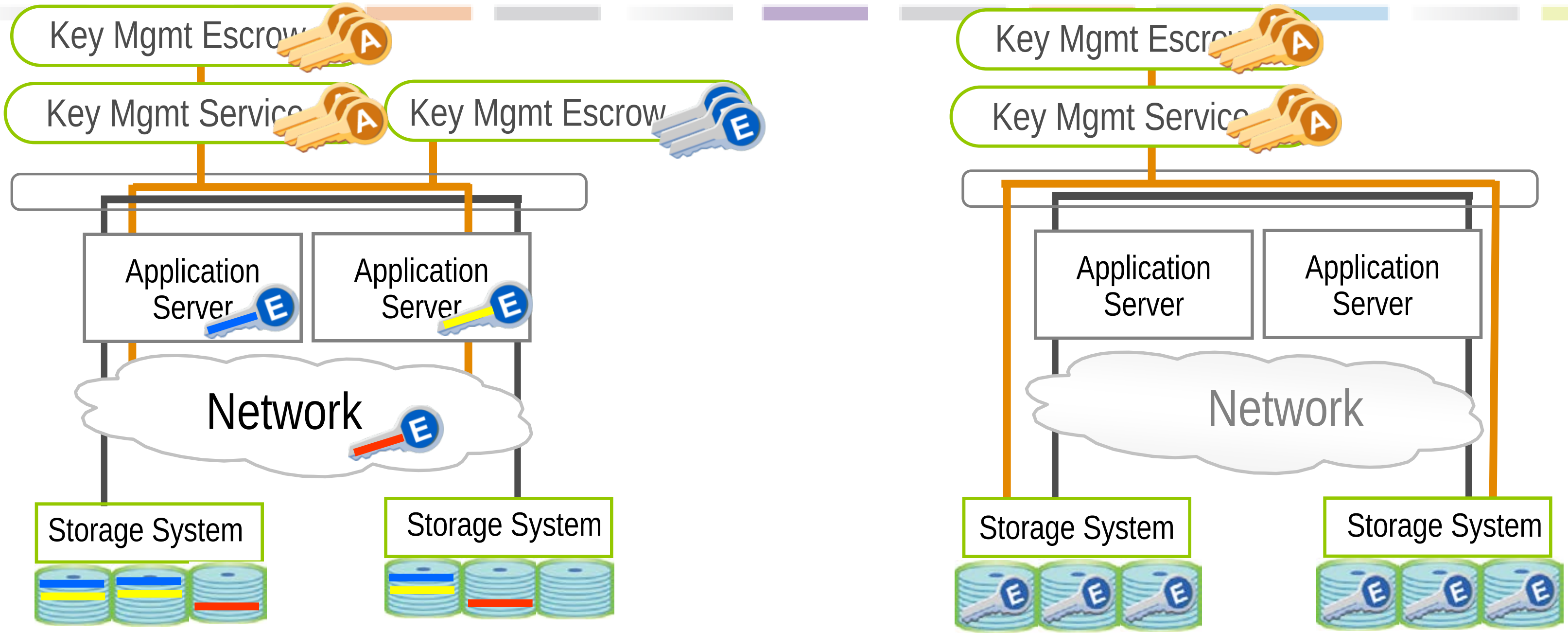
- Replace
- Repair
- Repurpose

**Power Off = Locked/Encrypted = Secure**

**Added "insurance": Crypto Erase**

- 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

# Key Management Simplification



Encrypting outside the drive

Encrypting in the drive

**Encryption key never leaves the drive. No need to track or manage …**

**BUT, YOU STILL MANAGE THE AUTHENTICATION KEYS (drive locking),**

**to protect against loss or theft (for just crypto erase, no authentication key needed)**

- **To recover data from a drive:**
  - ***Only need the Authentication Key and the drive***
  - Don’t need to escrow the encryption key to maintain data recoverability
  - Don’t need to track encryption key storage separate from data storage
  - Don’t need to be concerned with interoperability of encryption key storage and data

# 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

**New hardware acquisition (part of normal replacement cycle)**

# Performance Comparisons: HDD and SSD, software versus SED

SNIA™ Global Education

| MB/Sec | HDD: no encryption | HDD: S/W encryption | HDD: SED | SSD: no encryption | SSD: S/W encryption | SSD: 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/**

# ‘Hurdles’ to Implementing Encryption…

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

# 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<br>✓ Transparent to application developers and database administrators. No change to OS, applications, databases<br>✓ Data classification not needed to maintain performance |
| Solves Performance | ✓ No performance degradation<br>✓ Automatically scales linearly<br>✓ Can change keys without re-encrypting data |
| Reduces Cost | ✓ Standards enables competition and drive cost down<br>✓ Compression and de-duplication maintained<br>✓ Simplifies decommissioning and preserves hardware value for returns, repurposing |

# SNIA: Encryption of Data At-Rest
## *Step-by-step Checklist*

1. Understand Drivers
2. Classify Data Assets
3. Inventory Data Assets
4. Perform Data Flow Analysis
5. Choose Points-of-Encryption
6. Design Encryption Solution
7. Begin Data Re-Alignment
8. Implement Solution
9. Activate encryption

http://www.snia.org/forums/ssif/knowledge_center/white_papers

# The Steps (using SEDs)

1. Understand Drivers: **breach laws**
2. ~~Classify Data Assets~~
3. ~~Inventory Data Assets~~
4. ~~Perform Data Flow Analysis~~
5. Choose Points-of-Encryption: **drives**
6. Design Encryption Solution: **management**
7. ~~Begin Data Re-Alignment~~
8. Implement Solution: **SED phase-in**
9. Activate encryption: **automatic**

**Greatly Simplified Using SEDs**

- Data classification and asset inventory not required to support SEDs
- Higher layer encryption may additionally be mandated by regulations

# SED Superiority

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

- Scalable
- Interoperable
- Integrated
- Transparent

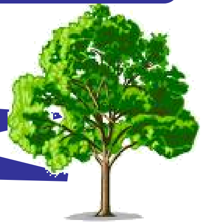
> "Many organizations are considering **drive-level security for its simplicity** in helping secure sensitive data through the hardware lifecycle from initial setup, to upgrade transitions and disposal"
>
> **Eric Ouellet**
> **Research Vice President**
> **Gartner**

# SOLID STATE DRIVES

## SSD ADVANTAGES

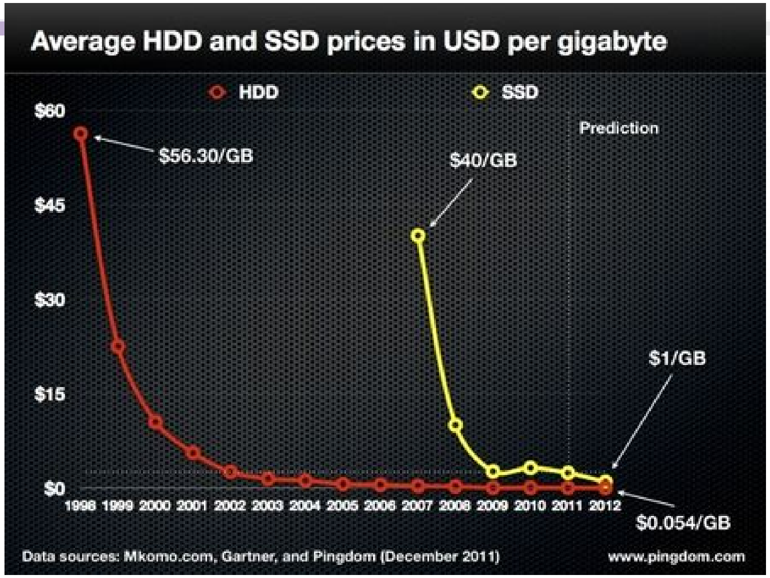
- Reduced maintenance times and cost → Save $$ on IT cost (TCO)
- Better performance → Faster booting and application launching
- More shock resistance → Shock proof
- More reliability (MTBF) → Fewer drive crashes
- Less power consumption → Energy efficient and **Green**

Save $$ on IT cost (TCO) + Faster booting and application launching + Shock proof + Fewer drive crashes + Energy efficient and **Green** = **Right Solution**



# HDD versus SSD “Cost” Comparison

## $$$/GB




http://www.tomshardware.com/news/ssd-hdd-solid-state-drive-hard-disk-drive-prices,14336.html

“… heat-assisted magnetic recording (HAMR) could push the (difference) even further….”

## http://www.diffen.com/difference/HDD_vs_SSD

Whereas hard drives are around $0.08 per gigabyte for 3.5", or $0.20 for 2.5", a typical flash SSD is about $0.80 per GB. This is down from about $2 per GB in early 2012.

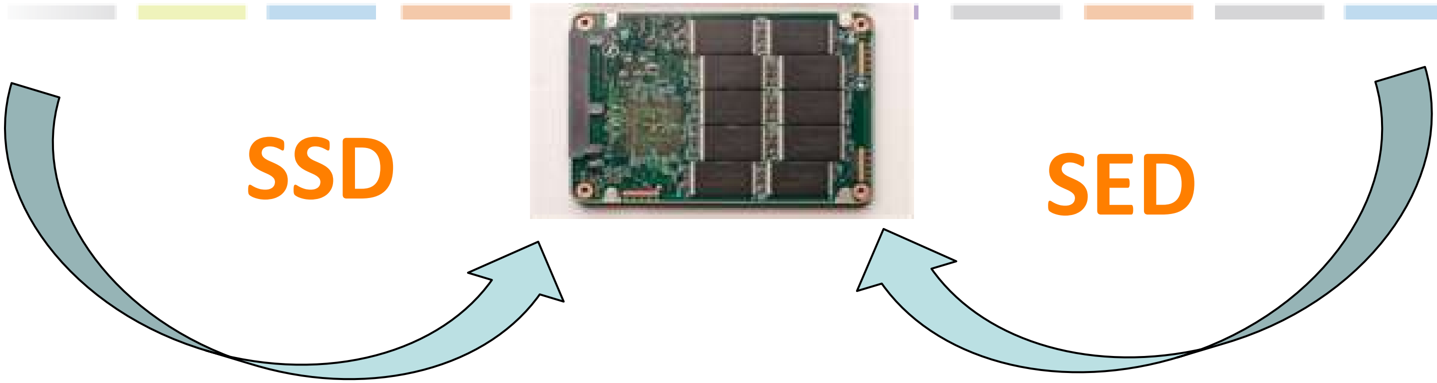
## $$$/IOPS

## IOPS are critical to the Enterprise

| | Hard Drive (HDD) 1x 15,000RPM 300GB SAS | Solid State (SSD) 300GB |
|---|---|---|
| In/Out Operations per Second (IOPS – Higher is Better) | 200~450 IOPS | 10,000~25,000 IOPS |
| Sequential Read/Write Speeds (MB/s – Higher is Better) | Read: 240MB/s Write: 210MB/s | Read: 510MB/s Write: 310MB/s |
| Random Read/Write Speeds (MB/s – Higher is Better) | Read: 2MB/s<br>Write: 5MB/s | Read: 60MB/s Write: 210MB/s |
| Sound | Low Hum, “clicky” sounds during Read and Write | Sound of Silence |
| Heat Output | Moderate | Very Low |
| Power Consumption (Idle/Load) | 14~17 Watts | 0.5~5 Watts |
| Sensitivity to Shock/Vibration | Yes w/ Data Loss | None |
| Sensitivity to Magnets | Yes w/ Data Loss | None |
| Fragmentation | Yes, degraded performance | None |
| Estimated Lifespan | 1.5 Million Hours | 2.0 Million Hours |

http://nutypesystems.com/rd-lab/ssd-vs-hdd-high-level/

# Solid-State Drive + Self-Encrypting Drive



## SIMPLE SOLUTION

- Reduced TCO
- Increased productivity
- Better Performance
- More shock resistance
- Better reliability
- Less power use
- Approaching price parity re: HDD
- Superior IOPS

- Simplified Management
- Robust Security
- Compliance “Safe Harbor”
- Cut Disposal Costs

- Scalable
- Interoperable
- Integrated
- Transparent

# Coughlin Reports: SED Marketing Forecasts

## Solid Security: The Rise of Self-Encrypting Solid State Drives

Thomas Coughlin

*Marketing Chair, SNIA Solid State Storage Initiative*
*President, Coughlin Associates*

**2011**

## Self-Encrypting Drive Marketing and Technology Report

Thomas Coughlin and Walt Hubis

**2015**

*http://www.tomcoughlin.com/techpapers.htm*

# SEDs are *already* ubiquitous worldwide

**~100% of all new, office and enterprise quality, Solid State Drives (SSDs) are TCG Opal SEDs**

Due to the Data Sanitization Problem for Flash (Traditional erasure techniques fail)

**~100% of all Enterprise Storage (SSD, HDD, etc) are TCG Enterprise SEDs**

eg, All of Google's Storage of your data and data they have on you

Fast, safe, and effective cryptographic repurposing and disposal of storage devices; protect against data leakage

**100% of all Apple iOS devices are hardware SEDs for user data**

when iPhone or iPad password is set, that is the KEK (Key Encrypting Key)

**~100% Western Digital USB Hard Disk Drives (HDDs) are SEDs**

In case you lose your USB storage device

**~100% of ALL Office-Class Printers and Copiers in the world use SEDs**

To protect **against theft of what people have printed/copied**

**>>> Much smaller number of Personal HDDs are TCG Opal or SED**

But Microsoft Bitlocker supports "eDrive" which requires Opal 2.0 SEDs

**100% TCG Opal Drives also support the SATA Security Password (Hard Disk Password)**

No Software needed: already supported by BIOS/UEFI setup on nearly every laptop and PC in the world

**Note:** Newest fastest solid state drives, such as NVMe, are already commercially available as TCG SEDs. Standardization details are currently being handled by the TCG Storage Workgroup.

# Factors Influencing Accelerated SED Adoption

SNIA
Global Education

AES/TCG in Controllers

All Channels/Models SED Capable

Diminishing/Zero Price Difference

Awareness: Breach Notification Exemption Compliance

# Saint Barnabas Health Care System: Case Study

- **Organization**
  - New Jersey's largest integrated healthcare system
    - 25 functional facilities total
  - Provides treatment for >2M patients/year
  - 18,200 employees, 4,600 doctors

- **Environment**
  - 2380 laptops
  - Adopted SED as standard for desktops this year (2011),
    - used by healthcare professionals and executives
    - distributed across 25 functional facilities
  - Protecting PII/PHI/diagnostic information
  - HP shop using Wave-managed Hitachi SEDs

BARNABAS HEALTH

# Case Study

- **Barnabas Health:**
  - **New Jersey’s largest integrated health delivery system**
  - **Implemented SEDs in 2380 laptops used by doctors, nurses, administrators and executives across 25 facilities**
  - **Will be encrypting 13,000 desktops used is the hospitals, via the asset lifecycle process in 4 years, 400 units expected to be done this year.**
- **Key Findings:**
  - **24 hours faster deployment on average per user over previous software-based encryption**
  - **Negligible boot time versus up to 30 minutes to boot a PC with software encryption**

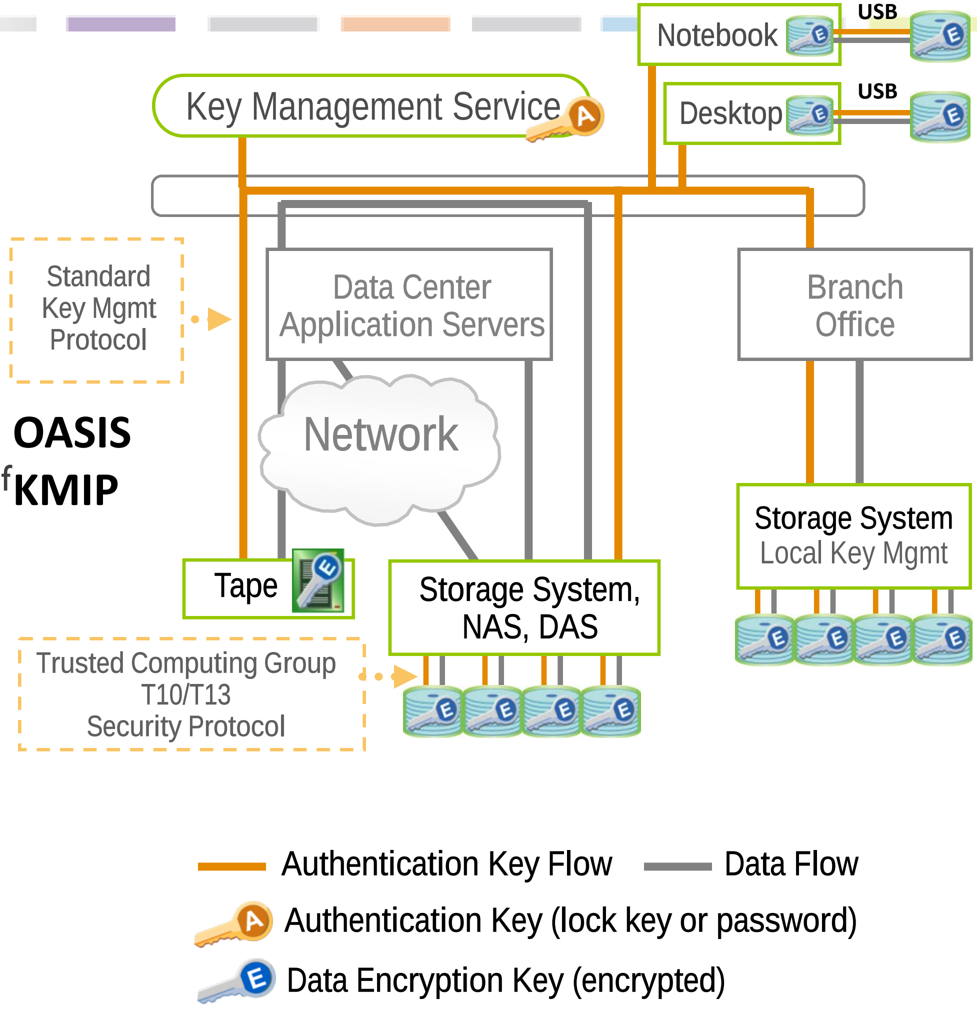
# Business Case

- Identify the data protection risks/requirements
  - Regulatory requirement for data protection
  - Safe harbor exemption
  - Intellectual property/ Proprietary information protection
- Build a business case
  - Market place analysis
  - Embed into the asset lifecycle program to manage expense

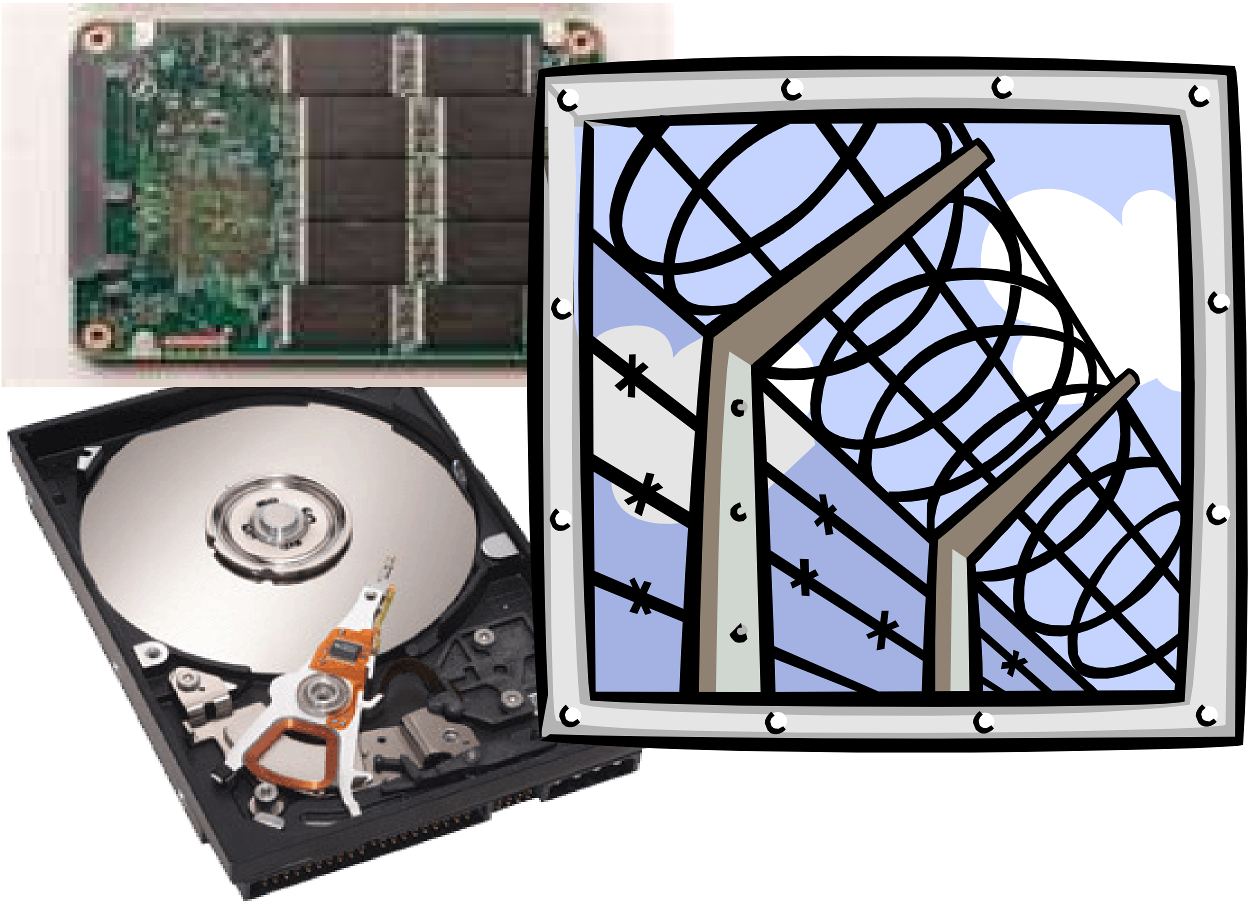
BARNABAS HEALTH

# Self-Encryption Everywhere

- **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


Notebook
USB
Desktop
USB
Key Management Service
Standard Key Mgmt Protocol
OASIS KMIP
Data Center Application Servers
Branch Office
Network
Tape
Storage System, NAS, DAS
Storage System Local Key Mgmt
Trusted Computing Group T10/T13 Security Protocol
Authentication Key Flow
Data Flow
Authentication Key (lock key or password)
Data Encryption Key (encrypted)

# Thank You!



# Attribution & Feedback

The SNIA Education Committee thanks the following individuals for their contributions to this Tutorial.

## Authorship History

Dr. Michael Willett

Updates:

Trusted Computing Group

## Additional Contributors

Gianna DaGiau
Eric Hibbard
Anne Price
Robert Thibadeau
Tom Coughlin

*Please send any questions or comments regarding this SNIA Tutorial to **tracktutorials@snia.org***