SNIA

Education

SELF-ENCRYPTING STORAGE

Michael Willett, Wave Systems
and WillettWorks Technology

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA.
- 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

SELF-ENCRYPTING STORAGE

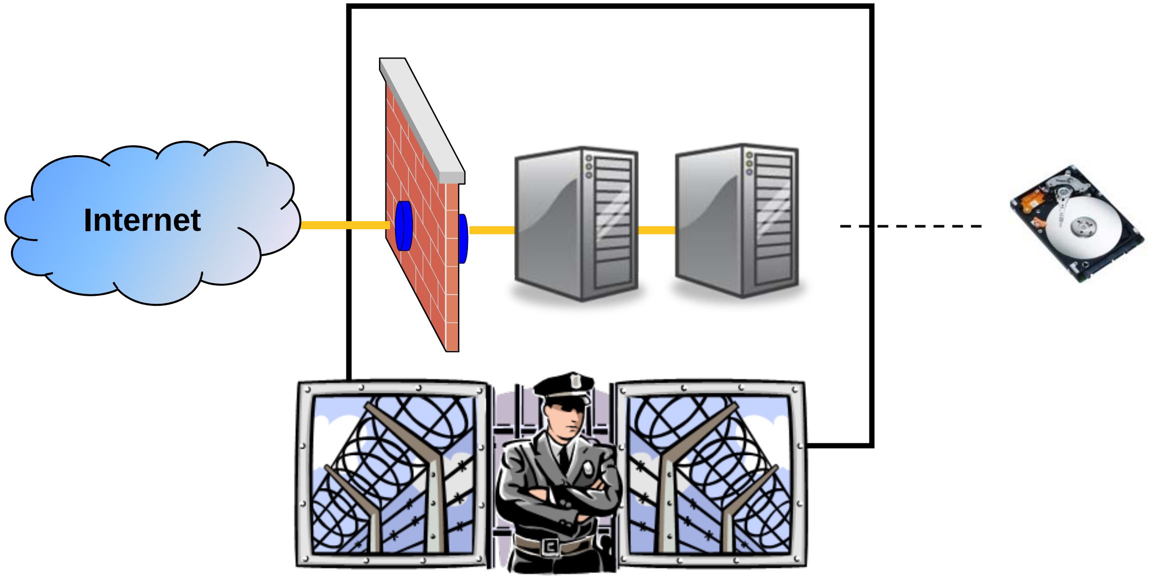
Data security is top of mind for most businesses trying to respond to the constant barrage of news highlighting data theft and security breaches. Combined with litigation risks, compliance issues and pending legislation, companies face a myriad of technology and products that all claim to protect data-at-rest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

The disk drive industry has standardized and is now deploying innovative, simple and powerful technology intended to secure data where it lives – in storage. This tutorial will give storage users and managers a look at emerging **drive-level self-encryption technology (both HDD and SSD) from notebook PCs to the data center** that provide a more secure storage foundation and compare that technology with alternate storage encryption methods, including: host-based, appliance, network fabric, and controller-based.

Check out SNIA Tutorial:

Cryptography Deciphered!

IT Security Today

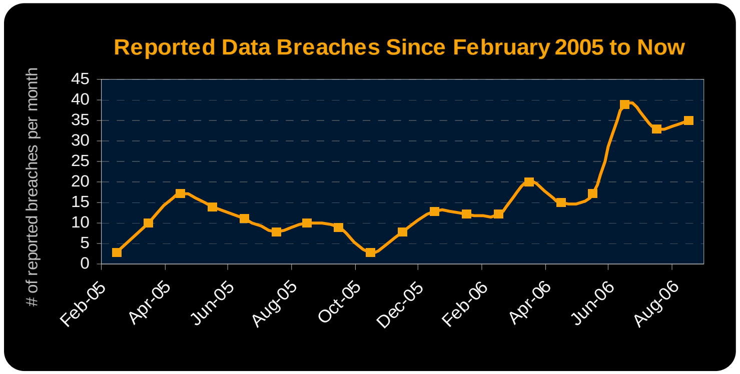


- Corporations spend millions to protect their networks, devices & data…
    - Physical security, firewalls, intrusion detection, etc…

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

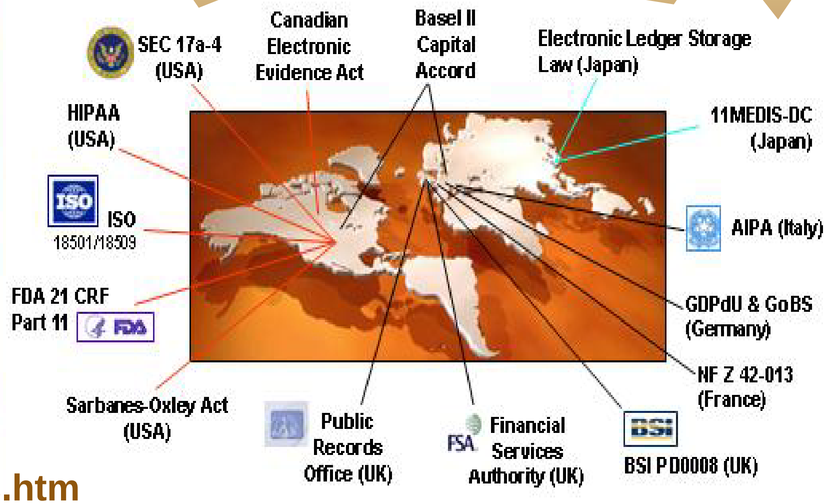
The Problem…

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 record)

$6.65 Million Per Incident



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

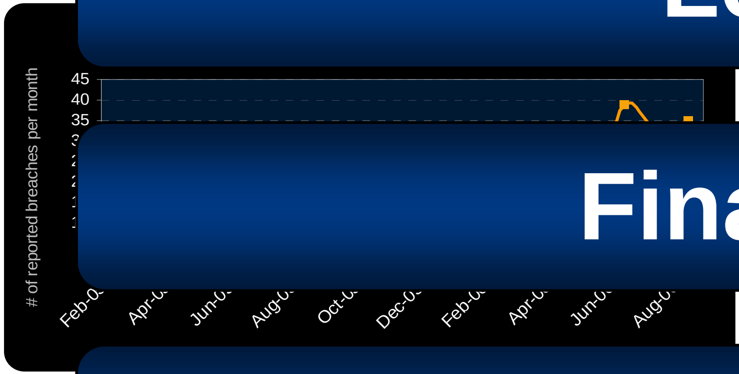
The Problem…

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

Legal

Financial

Reputation



reach was $6.65 million per affected corporation ($202 per record)

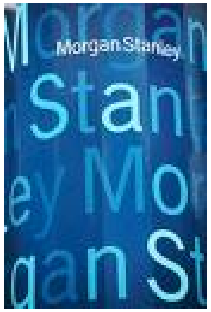
ncident

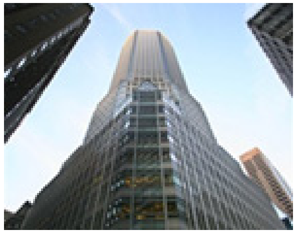
(USA)
Electronic Evidence Act
Capital Accord
ger Storage Law (Japan)
11MEDIS-DC (Japan)
AIPA (Italy)
GDPdU & GoBS (Germany)
NF Z 42-013 (France)
BSI PD0008 (UK)
Financial Services Authority (UK)
FSA
Public Records Office (UK)
Sarbanes-Oxley Act (USA)
FDA 21 CRF Part 11
FDA

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

Who is demanding a solution… ?

6 new bills on security breach, privacy, theft

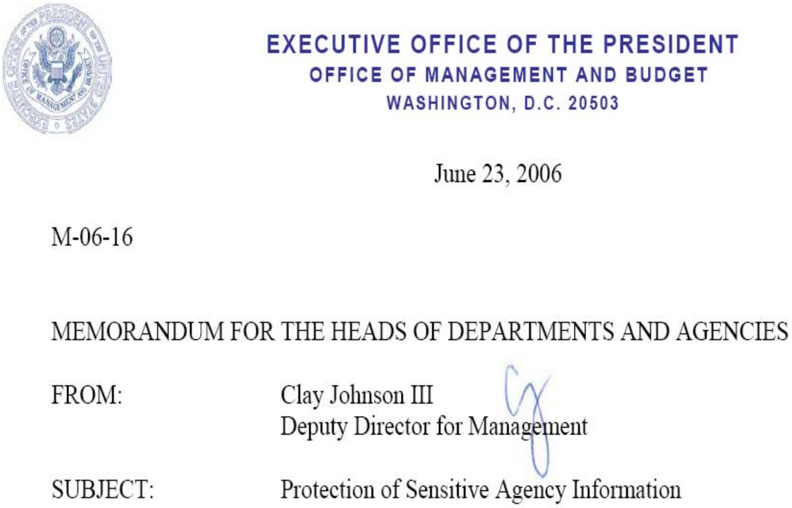




HIPAA COMPLIANT

(Requires FIPS-140 Compliance)

44+ states have passed breach notification laws w/ encryption safe harbors



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

June 23, 2006

M-06-16

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

FROM: Clay Johnson III
Deputy Director for Management

SUBJECT: Protection of Sensitive Agency Information

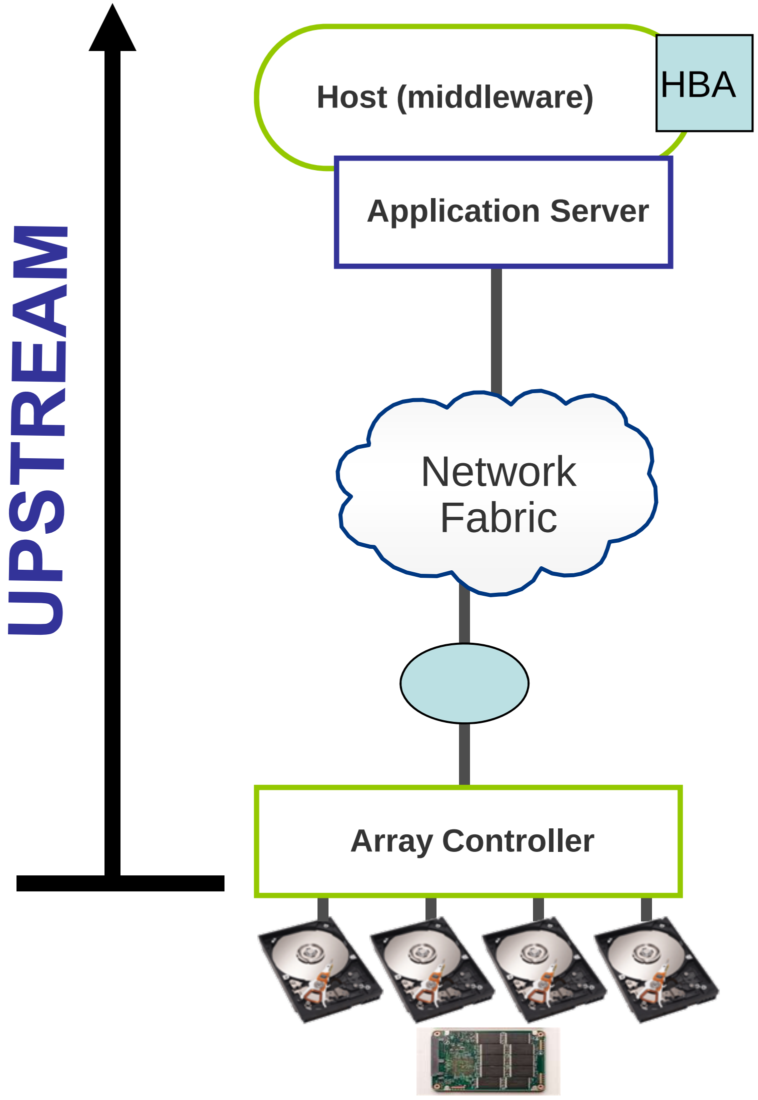
Why Encrypt Data-At-Rest?

- Compliance
  - **44+ 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**

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

Encryption can be done in a number of places…



Host middleware

Host HBA (h/w adapter)

Application

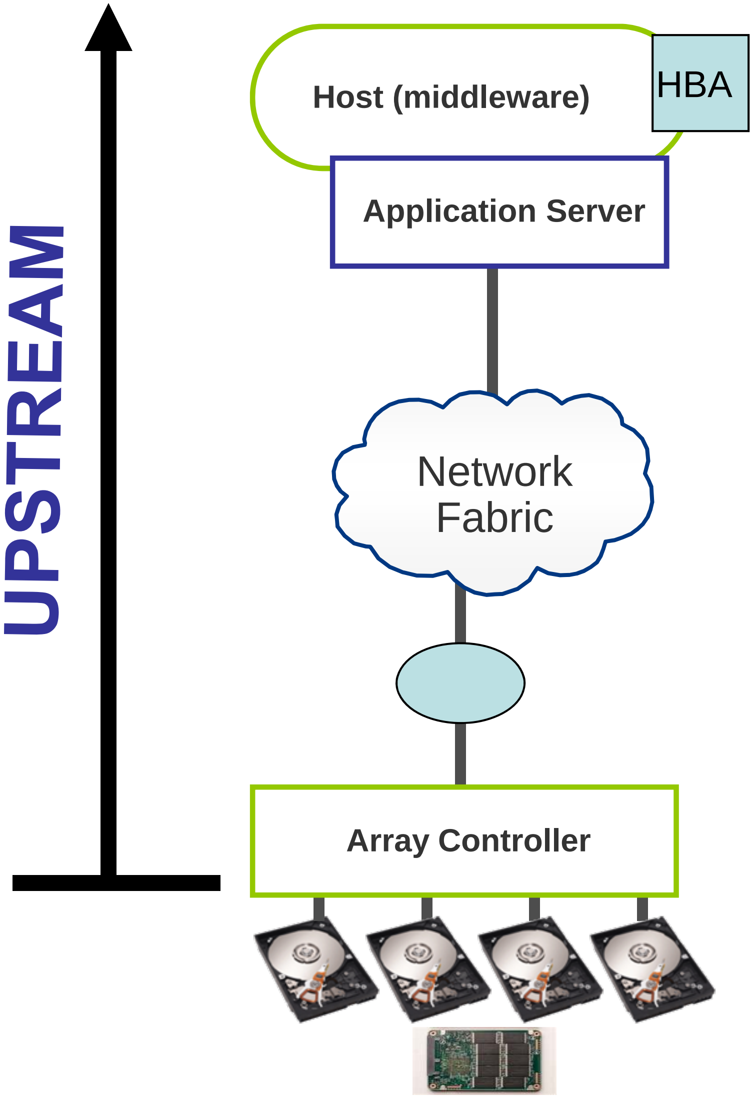
Switch

“Bump in the wire” appliance

Array controller

Drive (HDD, SSD)

Encryption can be done in a number of places…



Host middleware

Host HBA (h/w adapter)

Application

Switch

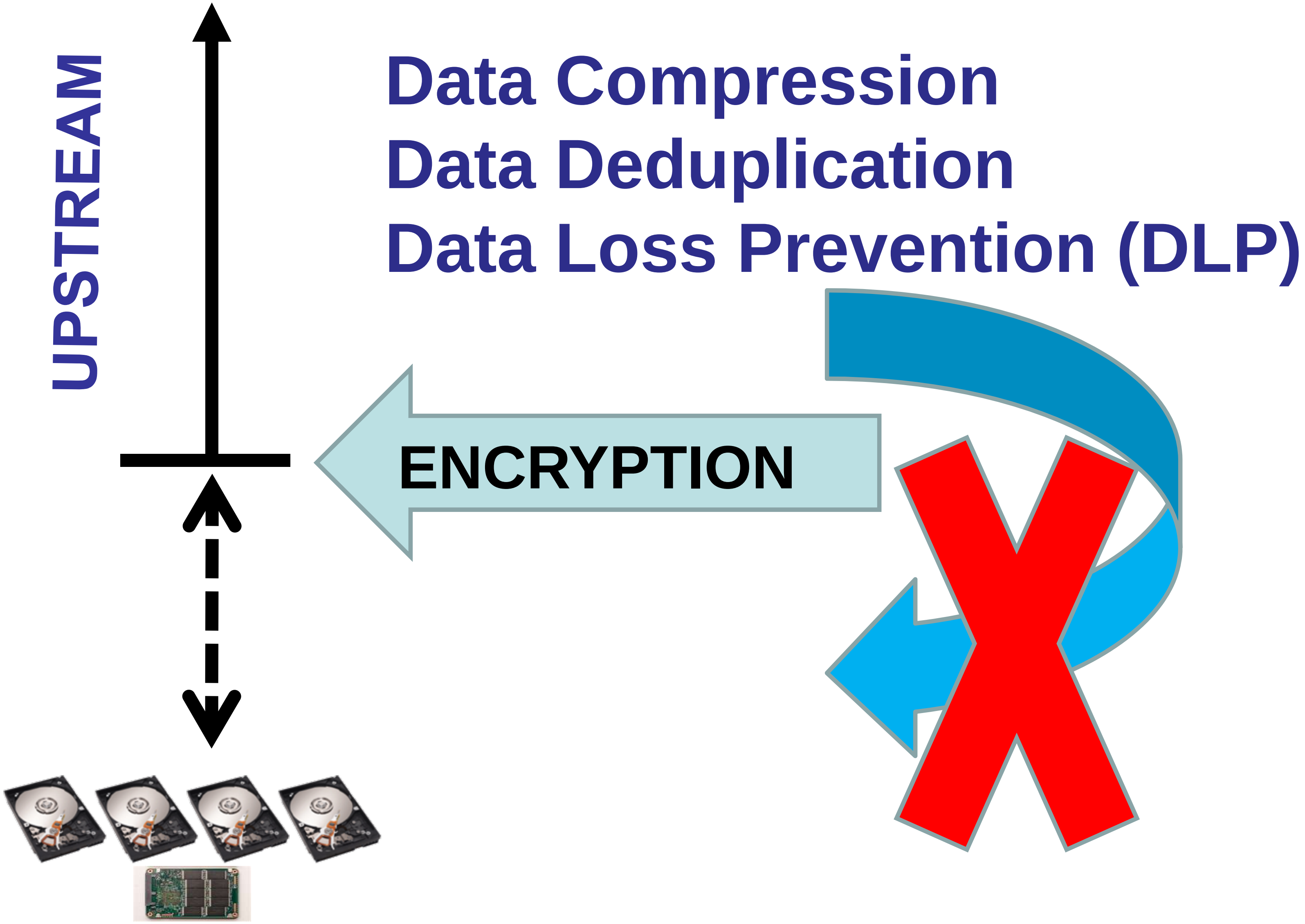
“Bump in the wire” appliance

Array controller

Drive (HDD, SSD)

DIFFERENT THREAT SCENARIOS

Encryption upstream can affect other processes



UPSTREAM

Data Compression

Data Deduplication

Data Loss Prevention (DLP)

ENCRYPTION

Why Security Directly in Drives?

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
  - Processing unit “welded” to storage unit
  - “Closed”, controlled environment
- Custom logic: faster, more secure operations
  - Inexpensive implementation of cryptographic functions
  - Complex security operations are feasible

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**

Self-Encrypting Drives Solve…

Purpose

- Protect data from exposure due to equipment loss
- Enable instant, secure erase of HDD/SSD **(delete on-board key)**

Closed encryption device

- Dedicated engine for full interface speed encryption
- Key generated by true RNG in drive
- Encryption cannot be turned off
- **Encryption Key never leaves the drive**
- Drive exposes an open interface for management of encryption & credentials
- Only signed firmware can be loaded onto drive

Storage System

2 Architectures

- Client (laptops, desktops) 3rd party software manages encryption
- Enterprise (arrays) Storage System manages encryption

Home Banking (or Remote Medical, or …)

Trusted Platform with Trusted Storage

- Multi-factor authentication: password, biometrics, dongles

- Secure/hardware storage of credentials, confidential financial/medical data

-Trusted life cycle management of personal information

- Integrity-checking of application software

- Cryptographic functions directly in storage

-Trusted/secure computation of high-value functions (protection from viruses/etc)

Home Banking (or Remote Medical, or …)

Breadth of Applications

Trusted Platform with Trusted Storage

- Multi-factor authentication: password, biometrics, dongles

- Secure/hardware storage of credentials, confidential financial/medical data

-Trusted life cycle management of personal information

- Integrity-checking of application software

- Cryptographic functions directly in storage

-Trusted/secure computation of high-value functions (protection from viruses/etc)

Trusted Storage Standardization

TRUSTED COMPUTING GROUP™

Published Storage Specifications

Joint Work – T10 (SCSI) and T13 (ATA)

TRUSTED SEND/IN

(Protocol ID = xxxx .....)

TRUSTED RECEIVE/OUT

SSD

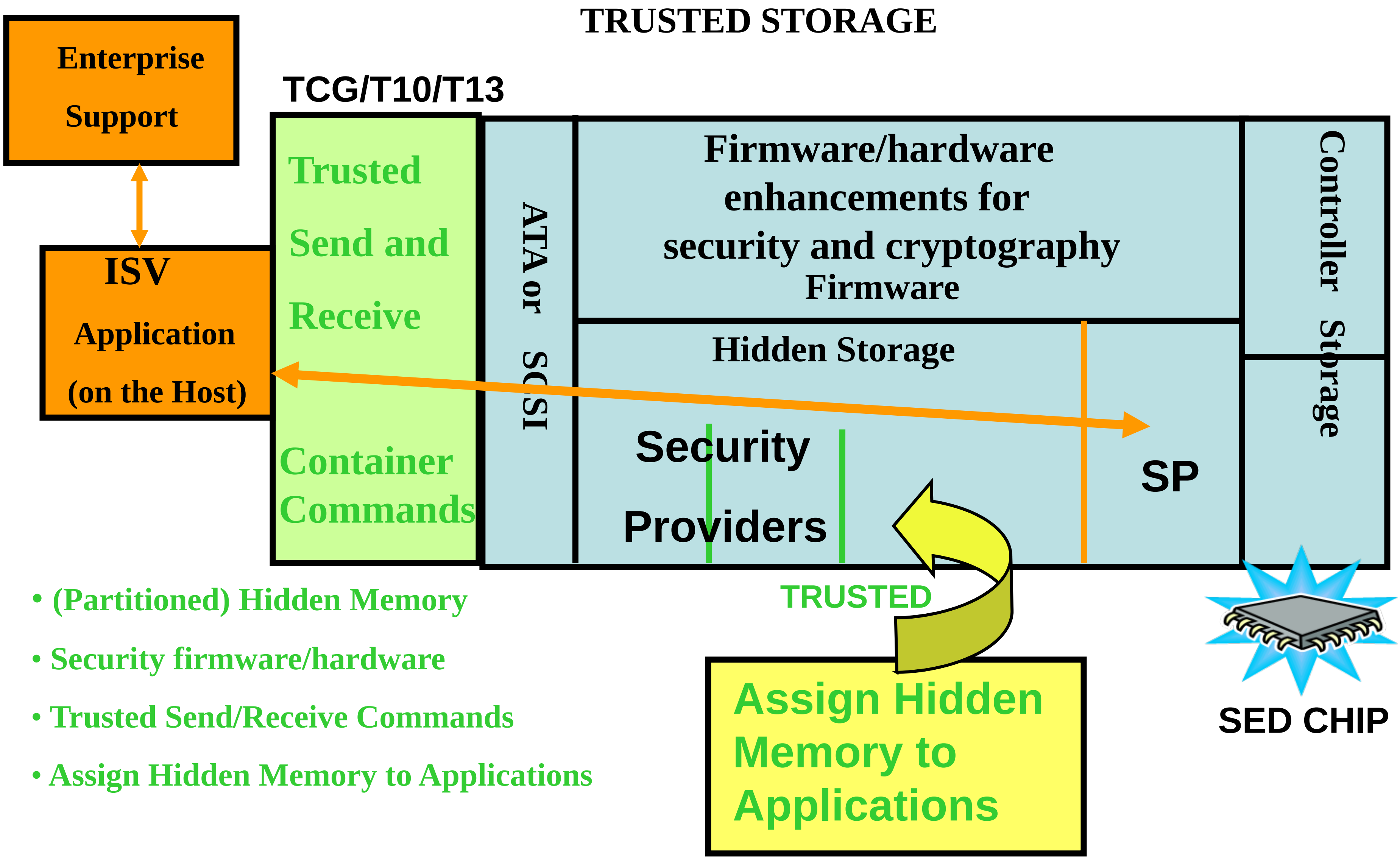
HDD

T10/T13 defined the "**container commands**"

TCG/Storage defining the "**TCG payload**"

Protocol IDs assigned to TCG, T10/T13, or reserved

Implementation Overview



TRUSTED STORAGE

Enterprise Support

ISV Application (on the Host)

TCG/T10/T13

Trusted Send and Receive Container Commands

ATA or SCSI

Firmware/hardware enhancements for security and cryptography

Firmware

Hidden Storage

Security Providers

SP

Controller Storage

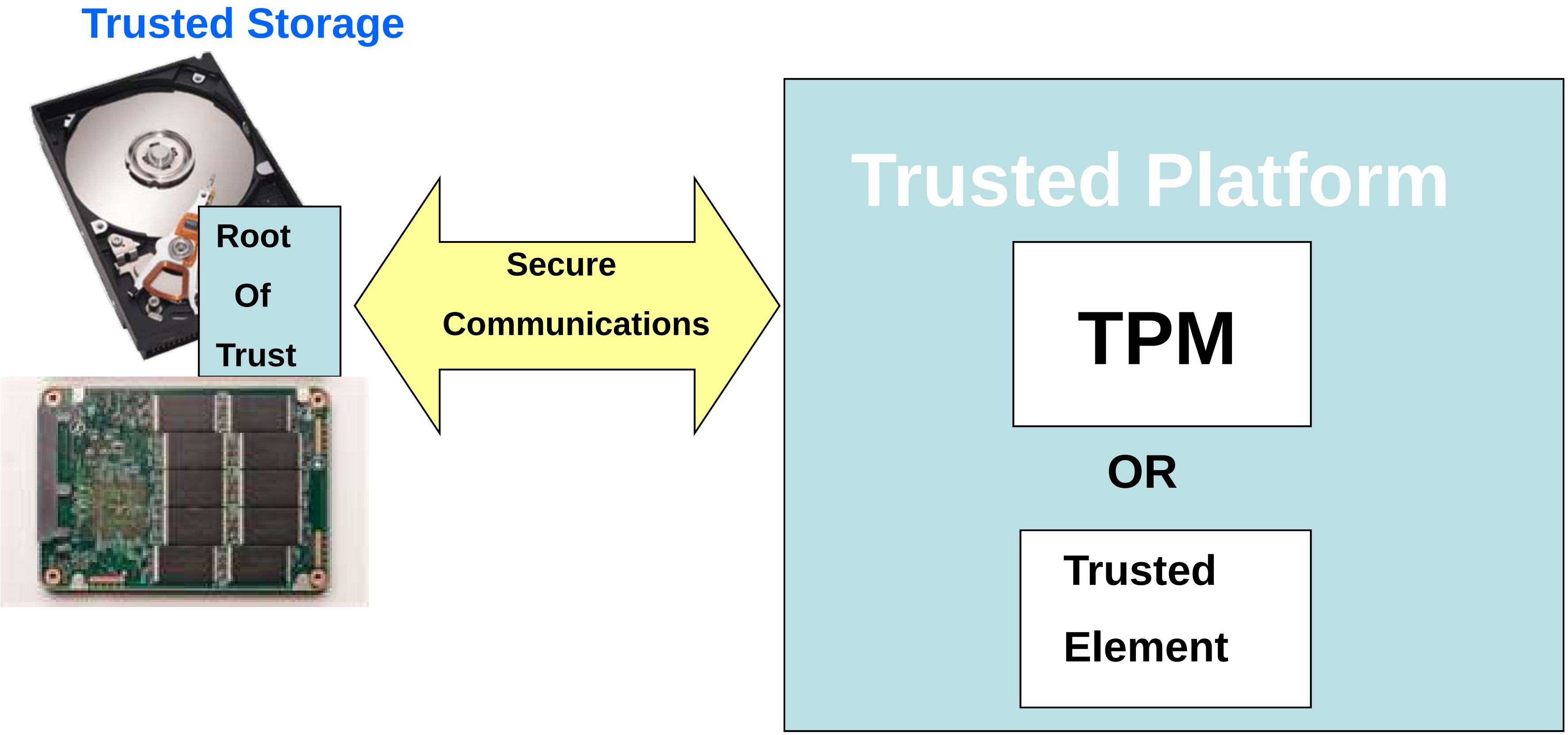
TRUSTED

Assign Hidden Memory to Applications

SED CHIP

- (Partitioned) Hidden Memory
- Security firmware/hardware
- Trusted Send/Receive Commands
- Assign Hidden Memory to Applications

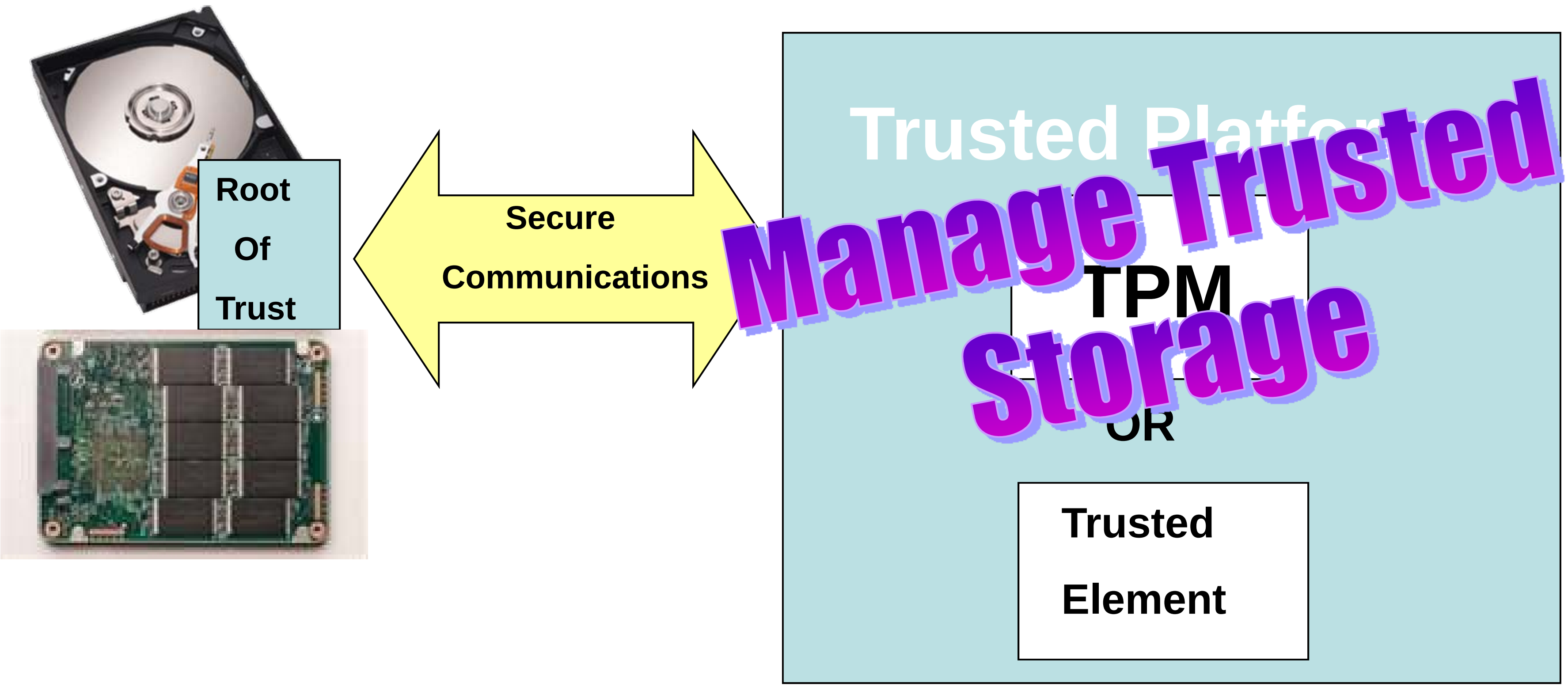
Trusted Storage with Trusted Platform



Life Cycle: Manufacture, Own, Enroll, PowerUp, Connect, Use, …

Trusted Storage with Trusted Platform

Trusted Storage



Root Of Trust

Secure Communications

Trusted Platform

TPM

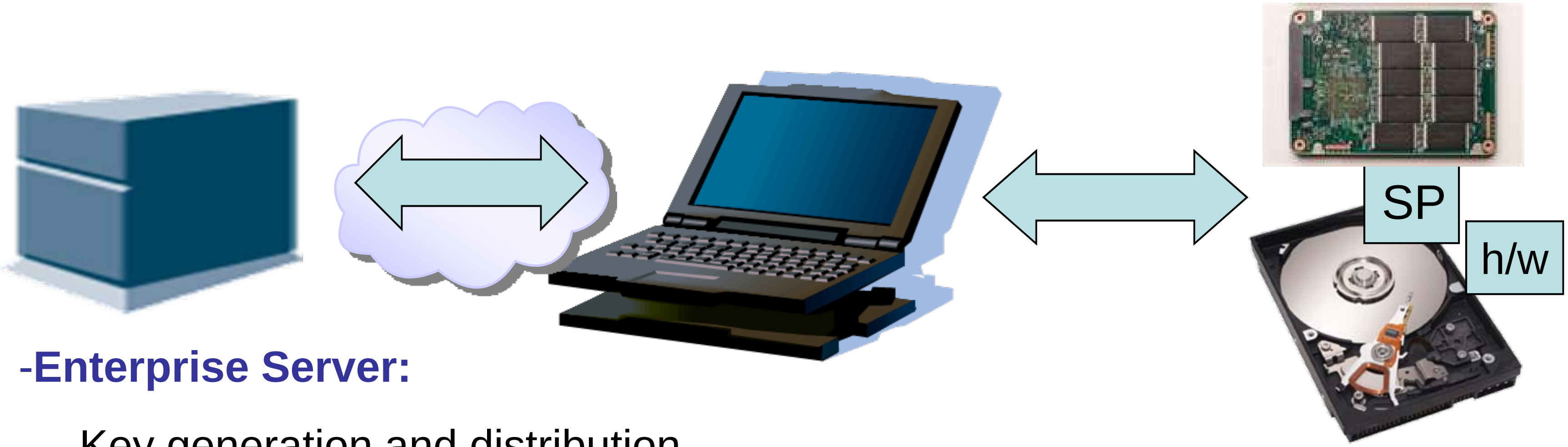
OR

Trusted Element

Manage Trusted Storage

Life Cycle: Manufacture, Own, Enroll, PowerUp, Connect, Use, …

Enterprise Management of Self-Encrypting Drives



Self-Encrypting Drive

-Enterprise Server:

Key generation and distribution

Key/Password archive, backup and recovery

-Laptop (Application):

Master/User passwords, multi-factor authentication, TPM support

Secure log-in, “Rapid Erase”

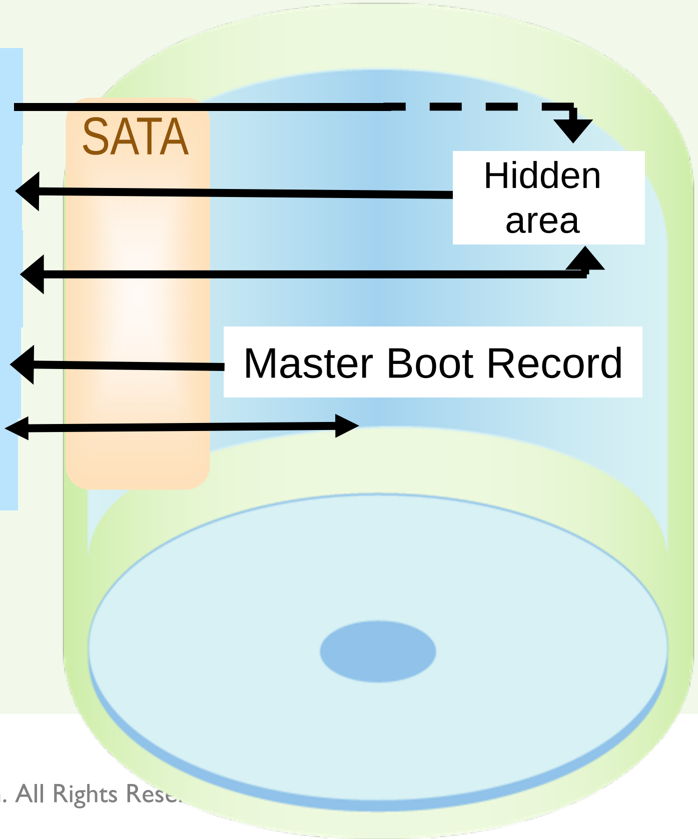
-Self-Encrypting Drive:

Disk or sector encryption, sensitive credential store, drive locking

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



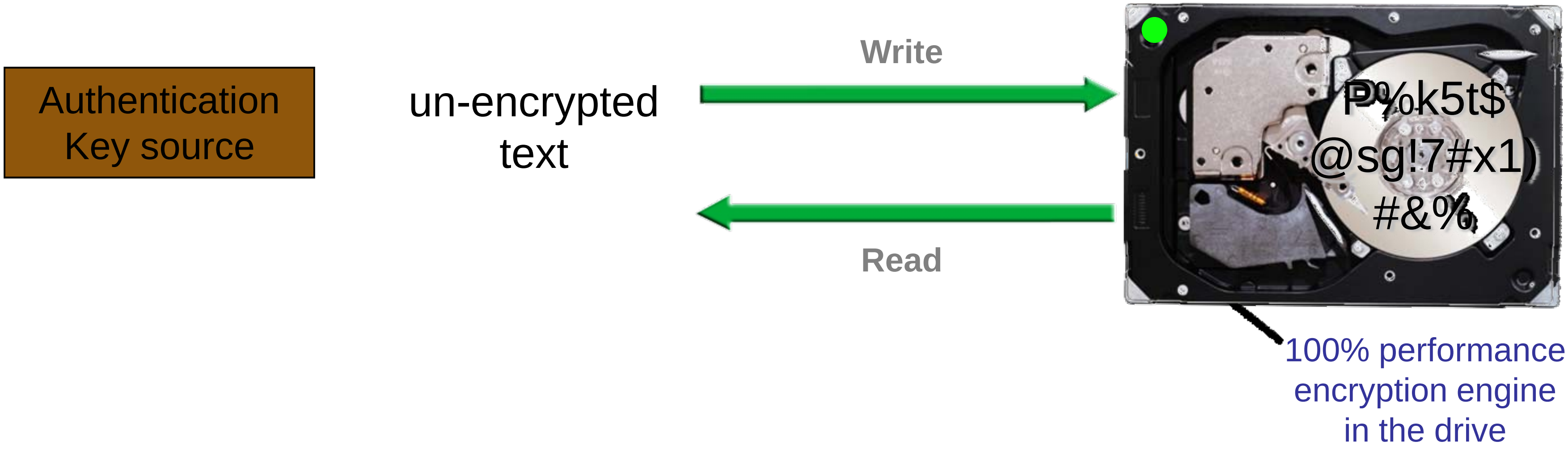
Self-Encrypting Drive Basics

The drive LOCKS automatically when powered OFF

The drive remains LOCKED when it is powered back ON

Authentication Key (Password) Unlocks the drive

Write and Read data normally while drive is unlocked



Authentication Key source

un-encrypted text

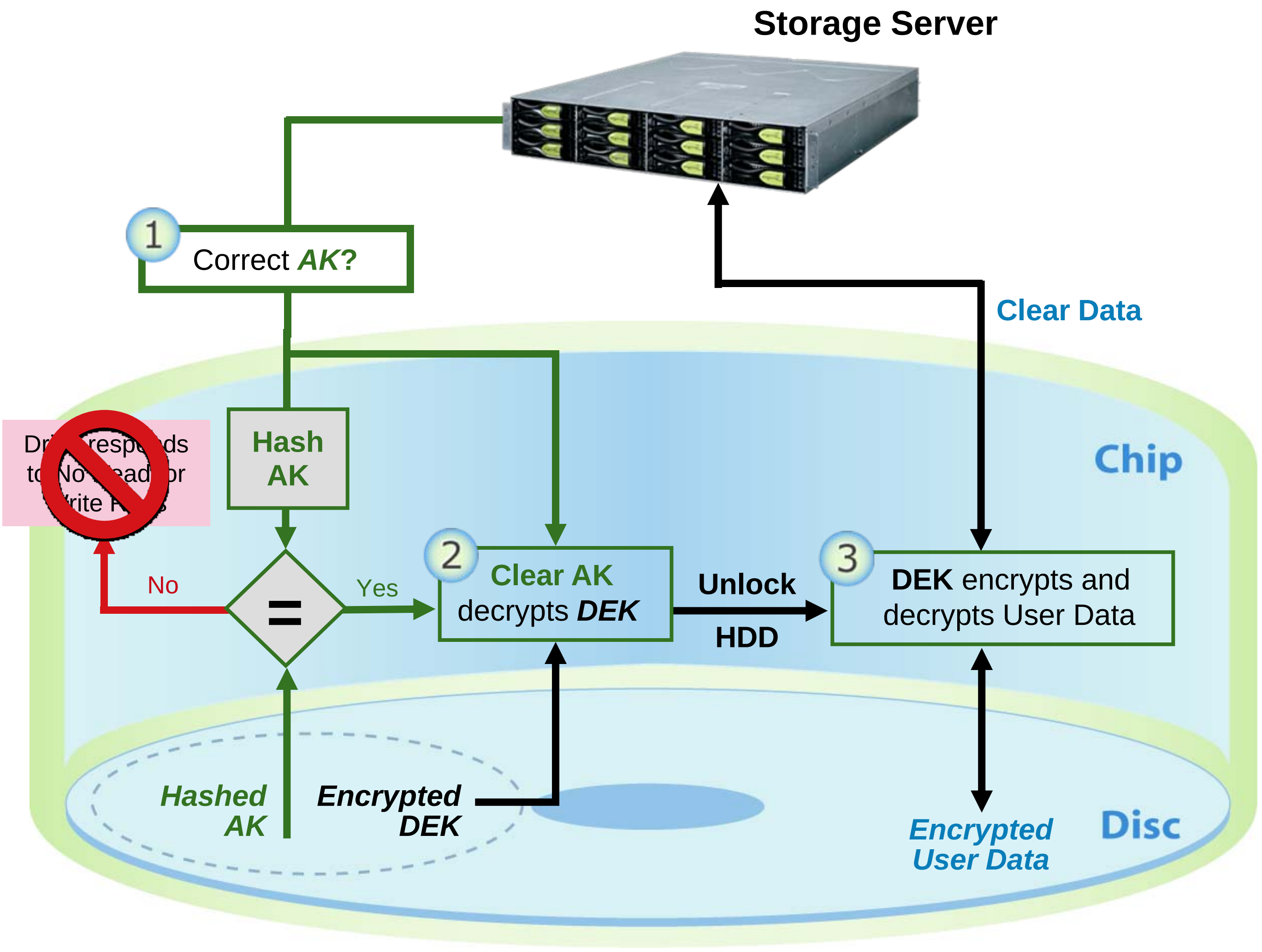
Write

Read

100% performance encryption engine in the drive

- Data protected from loss, disclosure

Authentication in the Drive



AK
Authentication Key

DEK
Data Encryption Key

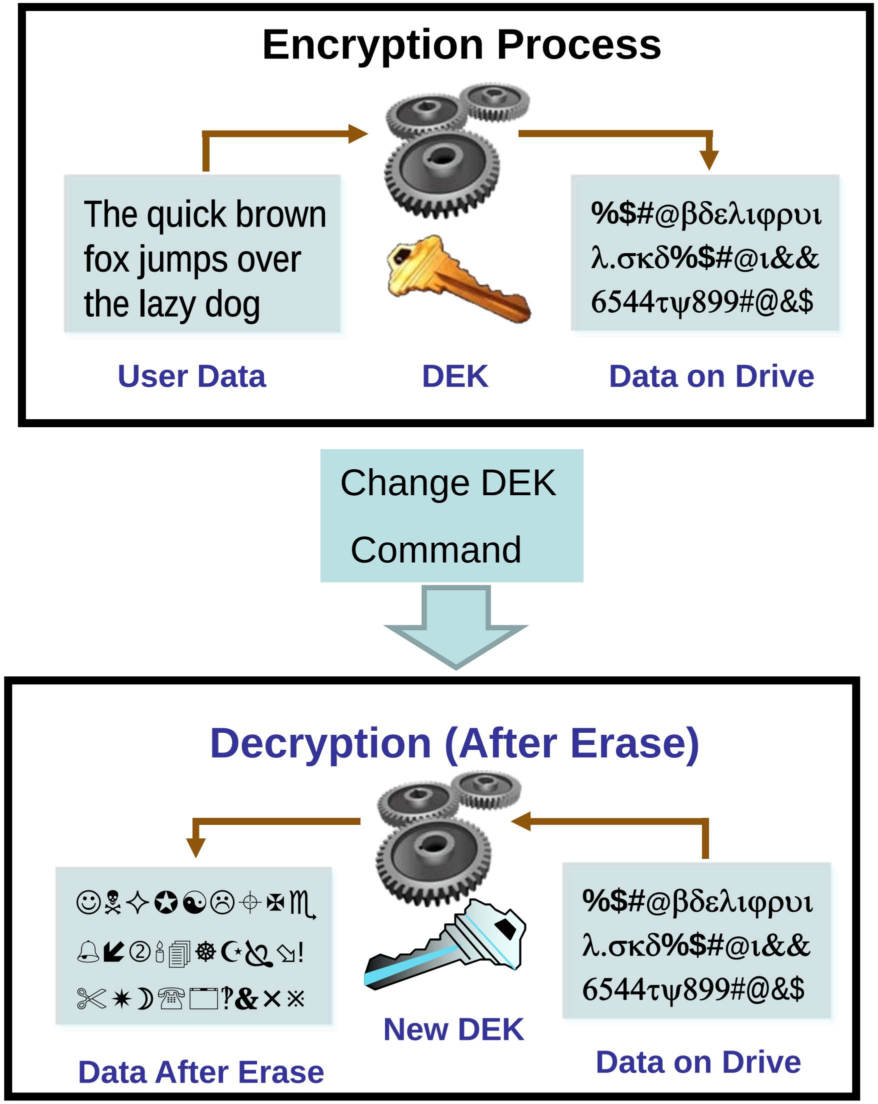
Cryptographic Erase

Description

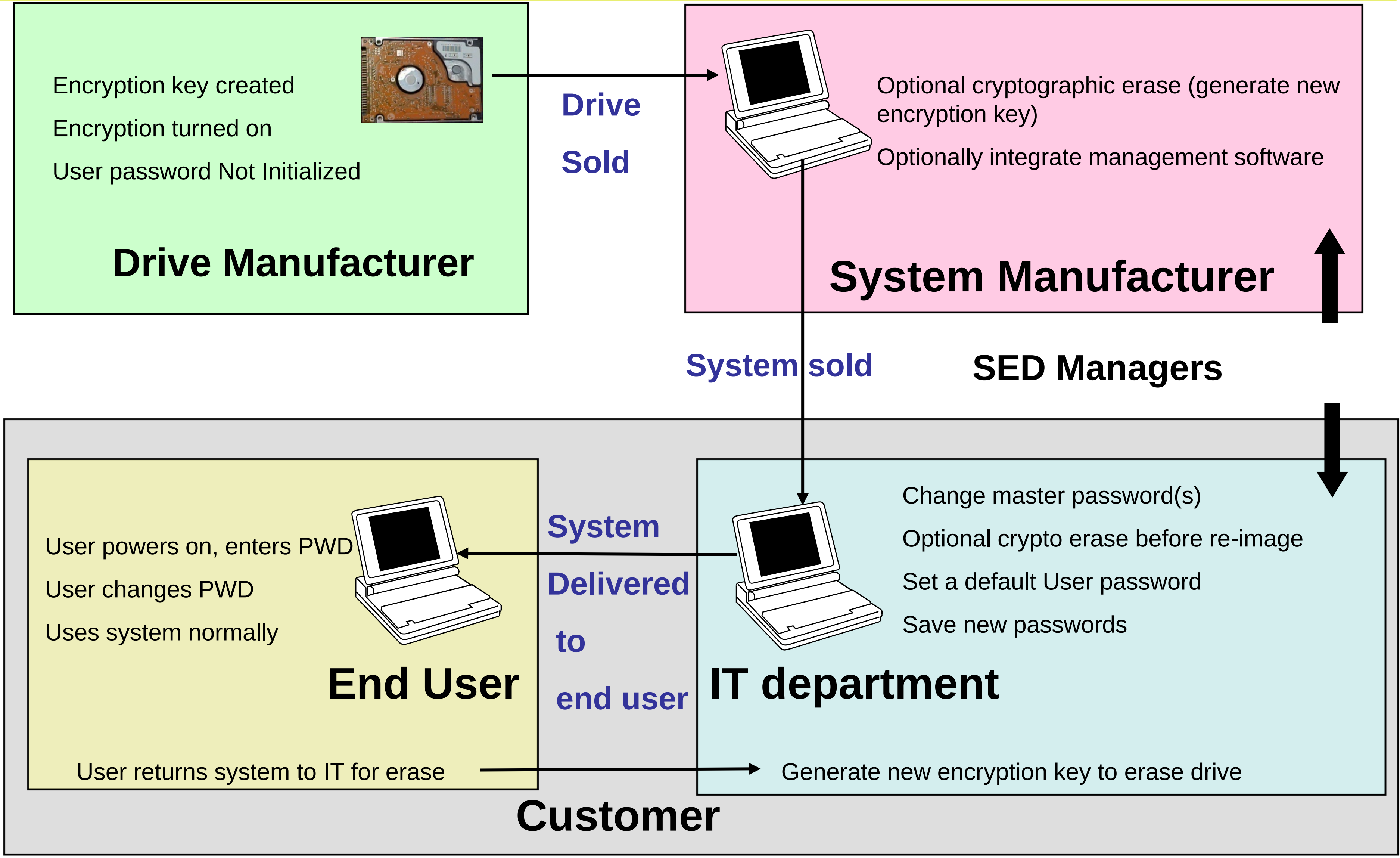
- Cryptographic erase changes the drive encryption key
- Data encrypted with previous key, unintelligible when **DEcrypted** with new key

Benefits

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



Client SED Deployment



Drive Manufacturer

Encryption key created

Encryption turned on

User password Not Initialized

Drive Sold

System Manufacturer

Optional cryptographic erase (generate new encryption key)

Optionally integrate management software

System sold

SED Managers

Customer

IT department

Change master password(s)

Optional crypto erase before re-image

Set a default User password

Save new passwords

System Delivered to end user

End User

User powers on, enters PWD

User changes PWD

Uses system normally

User returns system to IT for erase

Generate new encryption key to erase drive

‘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

No Performance Degradation

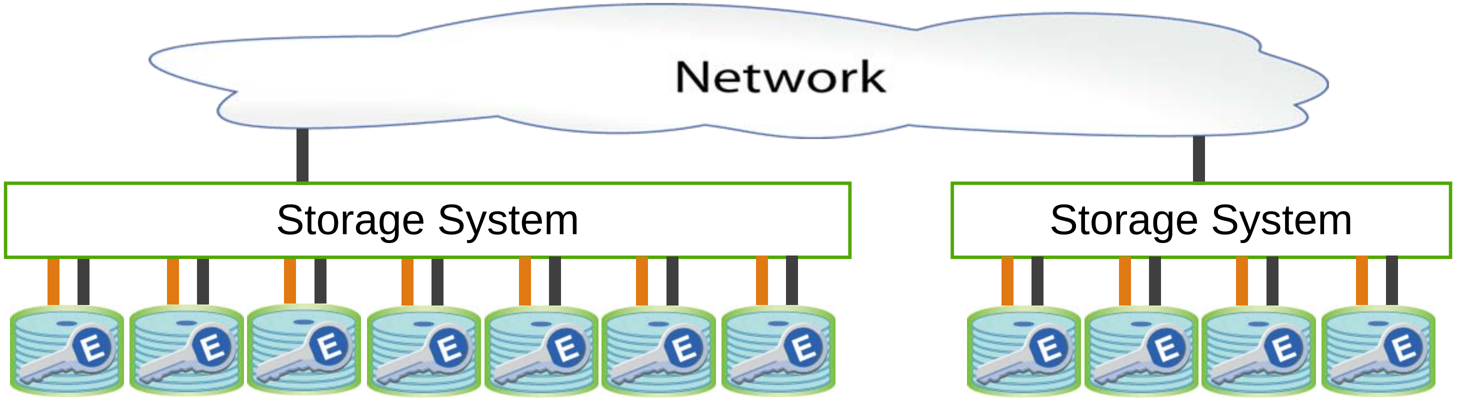
Encryption engine speed

Matches

Port's max speed

The encryption engine is in the controller ASIC

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

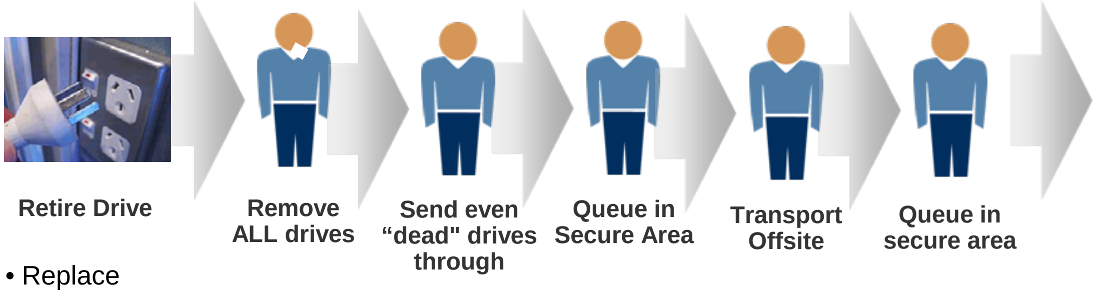
- 50,000 drives leave data centers daily
- Exposure of data is expensive - $6.65 million on average
- 90% of retired drives are still readable

(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

SECURE?

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_

How the Drive Retirement Process Works

Retirement Options

Retire Drive

- Replace
- Repair
- Repurpose

Drive Retirement is:

Expensive

Time-consuming

Error-prone

Overwriting takes
is no
n drive

gth
type

y

dding,

S E C U R E ?

hard drive data

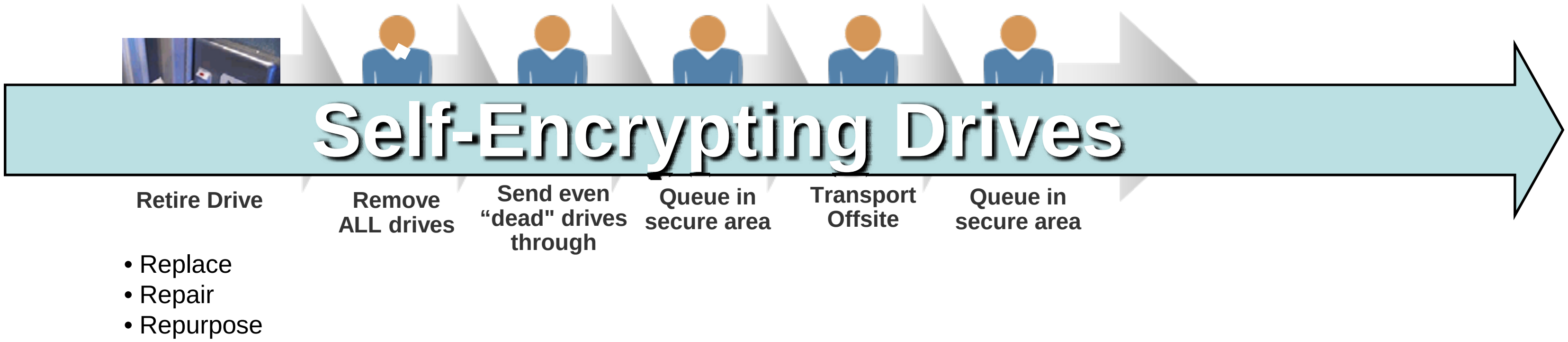
which lost a tape with 150,000 Social Security numbers stored at an Iron Mountain warehouse, October 2007[1]

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_

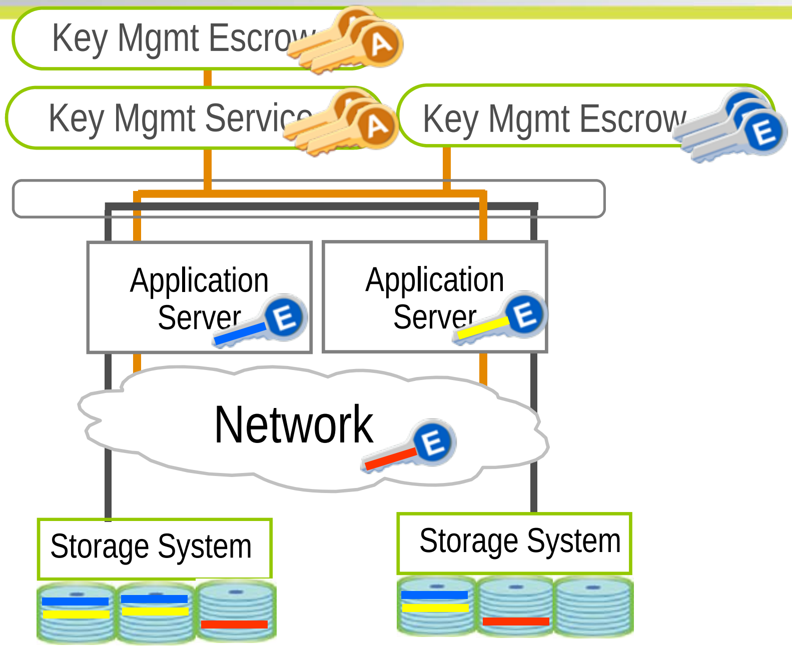
Drive Retirement: Self-Encrypting Drives



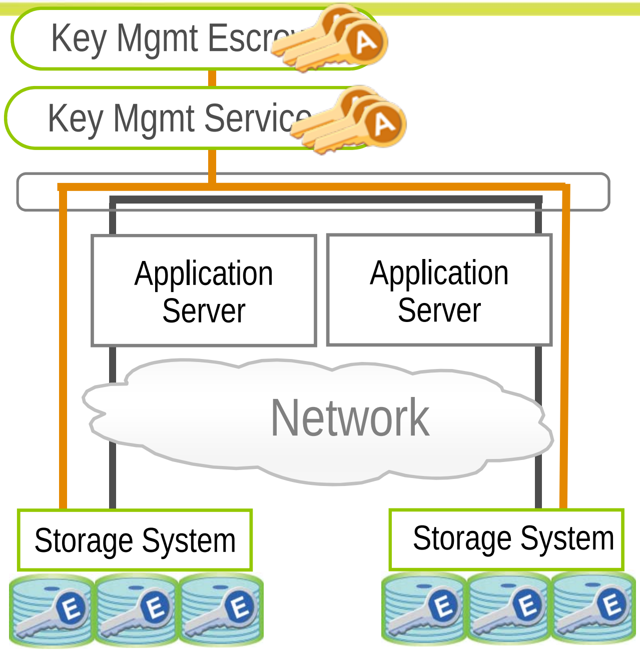
Power Off = Locked and Encrypted = Secure

- 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

Key Management Simplification



Encrypting outside the drive



Encrypting in the drive

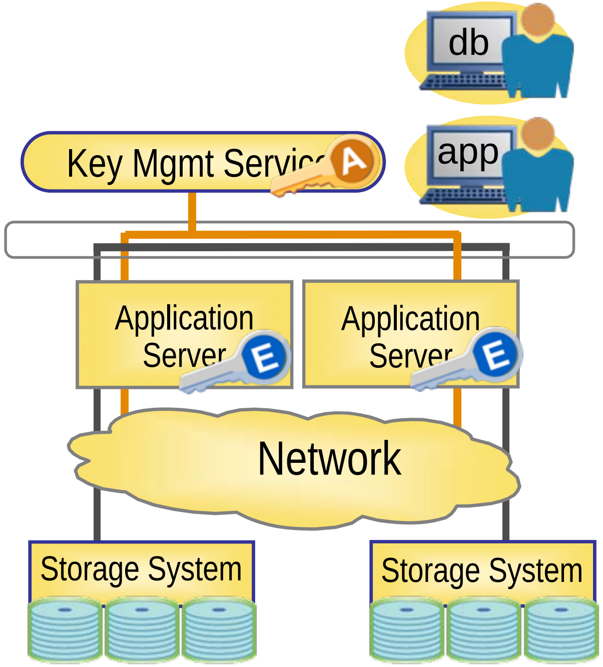
Encryption key never leaves the drive. No need to track or manage …

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

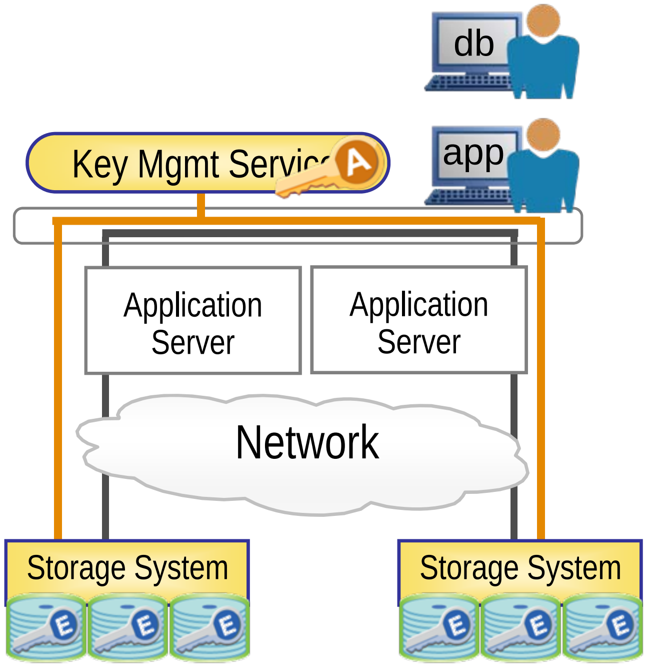
to protect against loss or theft (for just crypto erase, no authentication key needed)

- **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

Reducing Complexity for IT



Encrypting outside the drive

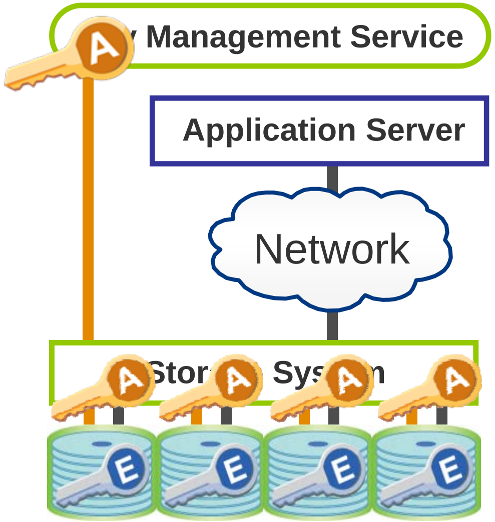


Encrypting inside the drive

- Application Developers: May need to change applications
- OS: May change if encrypting in a driver
- Encryption engine: May need separate hardware
- Network: Heavyweight encryption can impact performance
- Key Manager: Installed on existing server
- Storage System: Data compression & de-duplication affected

- Key Manager: Installed on existing server
- Storage System: Upgrade per schedule

Storage System Operations



At Initialization:

- Bring in new volume
- Set up Authentication Key

Power-up:

- Authenticate with the key source
- Pass key to the disk drive

After Power-up:

The storage system virtualizes the drives and provides:

- Data protection through RAID and copy services
- Availability through redundancy, failover drivers, robust error handling
- Capacity sharing through partitioning and network connectivity
- Management reporting
- Data compression and deduplication best applied BEFORE encryption

Reducing Security Costs

- **Initial acquisition costs:**
  - Integrated into standard products
  - Implemented per regular storage upgrade schedule
  - Standards-based, and all drive vendors are participating in TCG
  - The drive industry has long demonstrated standards promote competition which drives cost
  - Economies of scale enable incremental logic in the ASICs to remain a small portion of drive material costs
- **Reduce drive decommissioning and insurance costs**
- **Maintain ability to compress and deduplicate data**
- **Preserve drive hardware value**
  - Service, warranty, expired lease returns enabled
  - Drive repurposing enabled

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

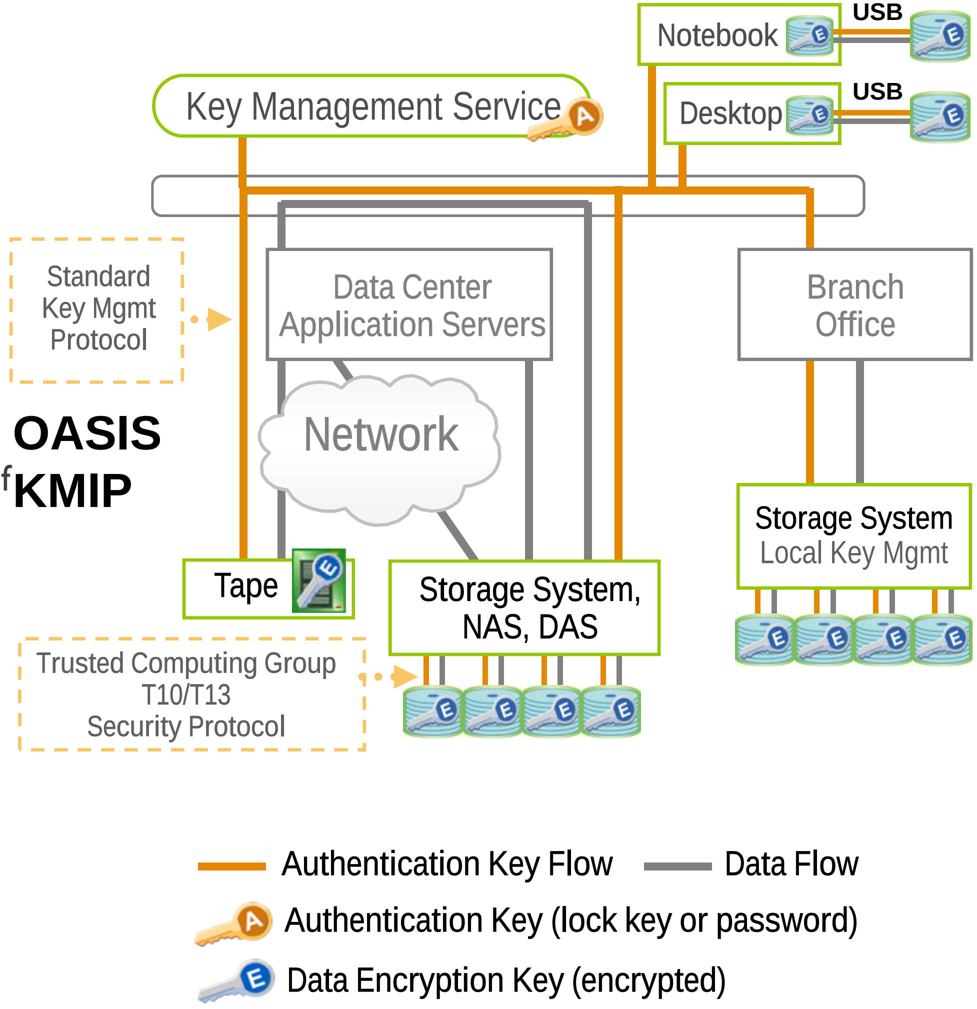
ISSUE: Hardware acquisition (part of normal replacement cycle)

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

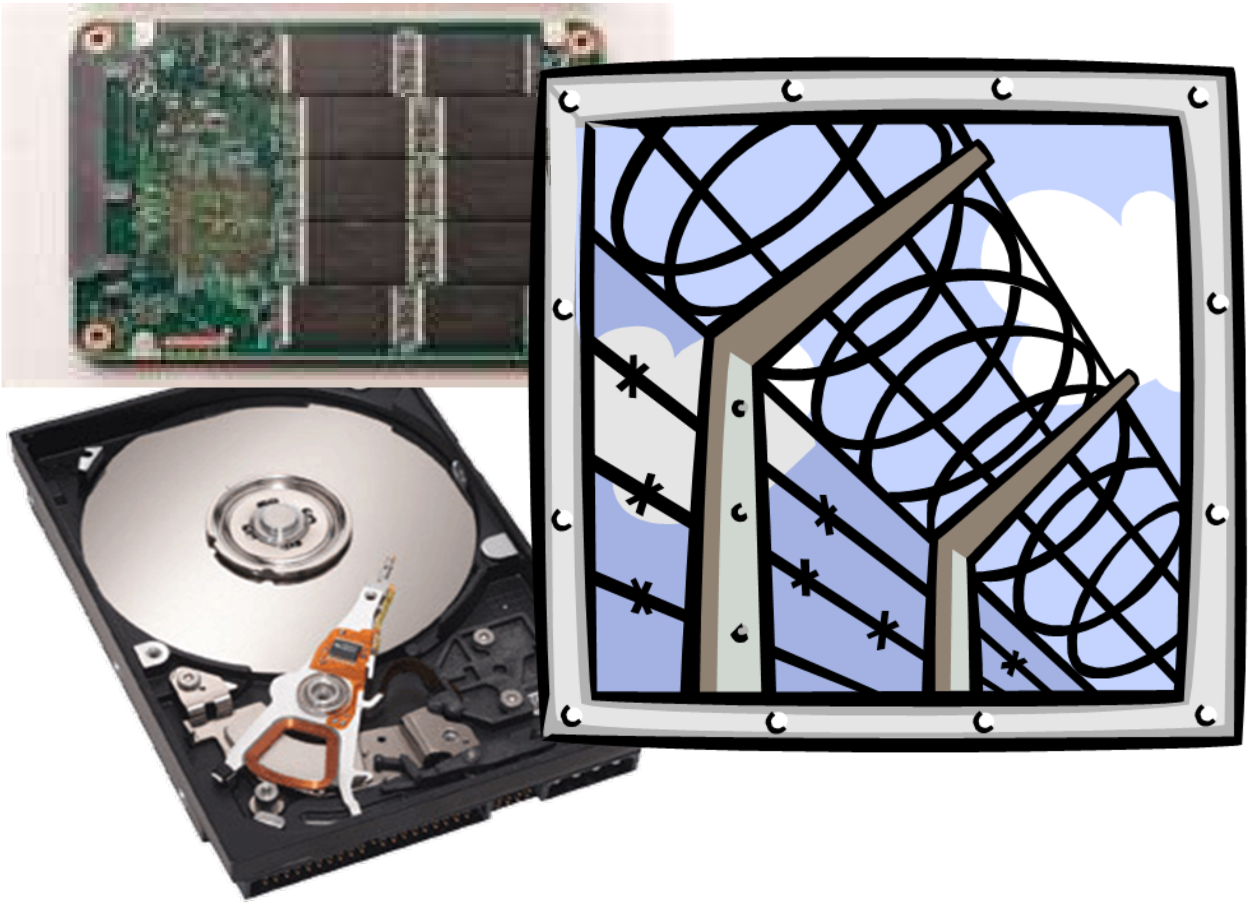
The Future: Self-Encrypting Drives

- **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



Notebook
USB
Desktop
USB
Key Management Service
Standard Key Mgmt Protocol
OASIS KMIP
Data Center Application Servers
Branch Office
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)

Thank You!



SNIA Security: Get Involved!

- SNIA Security Technical Work Group (TWG)
  - Focus: Requirements, architectures, interfaces, practices, technology, educational materials, and terminology for storage networking.
  - http://www.snia.org/tech_activities/workgroups
- Storage Security Industry Forum (SSIF)
  - Focus: Marketing collateral, educational materials, customer needs, whitepapers including the BCPs & Encryption of Data At-Rest (a Step-by-Step Checklist)
  - http://www.snia.org/forums/ssif

Q&A / Feedback

- Please send any questions or comments on this presentation to SNIA: tracksecurity@snia.org

Many thanks to the following individuals for their contributions to this tutorial.

- SNIA Education Committee

Gianna DaGiau
Eric A. Hibbard, CISSP, CISA
SNIA SSIF
Jason Cox

TCG Storage Use Case Examples

Self-Encrypting Drive

-Laptop Loss or Theft

-Re-Purposing

-End of Life

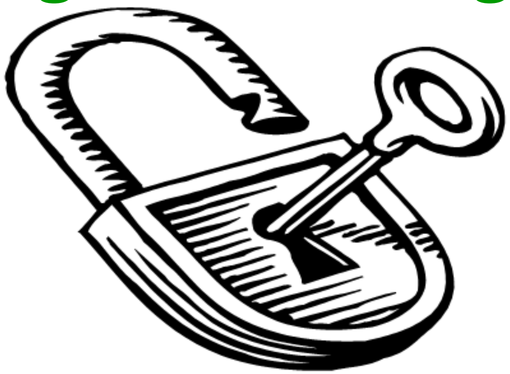
-Rapid Erase

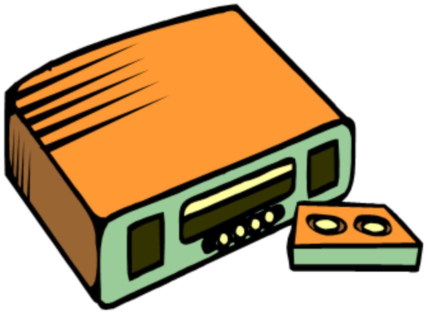
On-board Crypto Key Management

ALL Encrypted

Crypto Chip

DriveLocking/DrivePairing





Personal Video Recorders

Forensic Logging

DRM Building Blocks

TCG Storage WG Core Specification

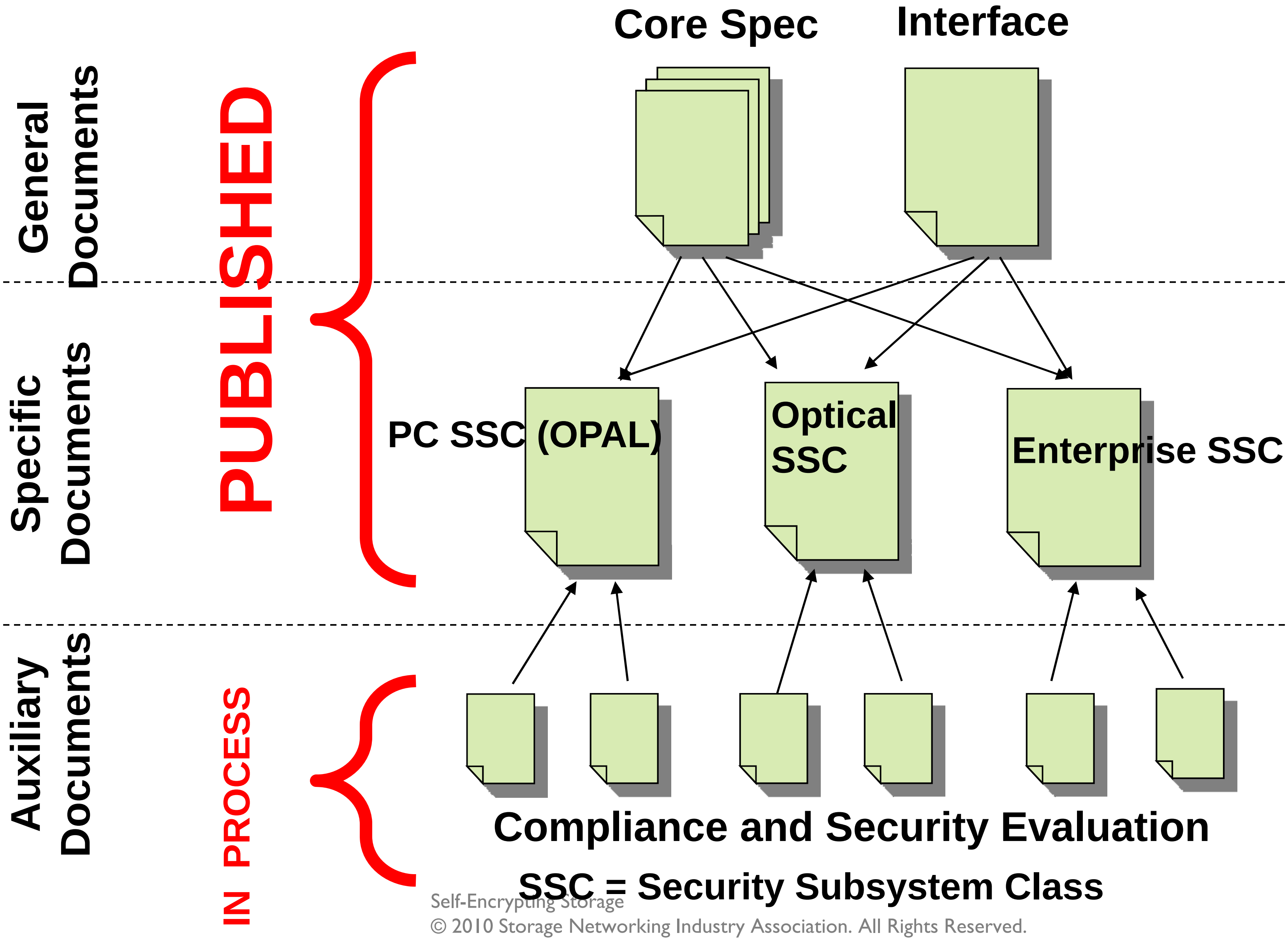
- **SPs** (Security Providers)
  - Logical Groupings of Features
  - SP = Tables + Methods + Access Controls
- **Tables**
  - Like "registers", primitive storage and control
- **Methods**
  - Get, Set – Commands kept simple with many possible functions
- **Access Control** over Methods on Tables

TCG Storage WG Core Specification

SIMPLE PROGRAMMING CONSTRUCTS

- **SPs** (Security Providers)
  - Logical Groupings of Features
  - SP = Tables + Methods + Access Controls
- **Tables**
  - Like "registers", primitive storage and control
- **Methods**
  - Get, Set – Commands kept simple with many possible functions
- **Access Control** over Methods on Tables

TCG Storage: Document Structure



SSC = Security Subsystem Class