

A silhouette of a person holding a large fishing net against a sunset sky. The person is in the foreground, holding the net which is draped across the sky. The background shows a sunset with orange and yellow light, and a line of trees on the horizon.

Seagate

**Drive Firmware
Security Overview**

Dave Anderson, Enterprise Storage

“Accept the security
breach or clean a litter
box.
Take your pick...”

Security is a Trade-Off ...!



Topics

1. Problem Statement:
Mitigate Firmware and Diagnostics related HDD attacks
2. Self Encrypting Drive Basics
3. Mitigating Methods
4. Parting Thoughts

SED Cryptography and Completeness

Self Encrypting Drive development brought clear recognition of need

Encrypting data is useless unless back doors into drive were locked

Firmware must be protected

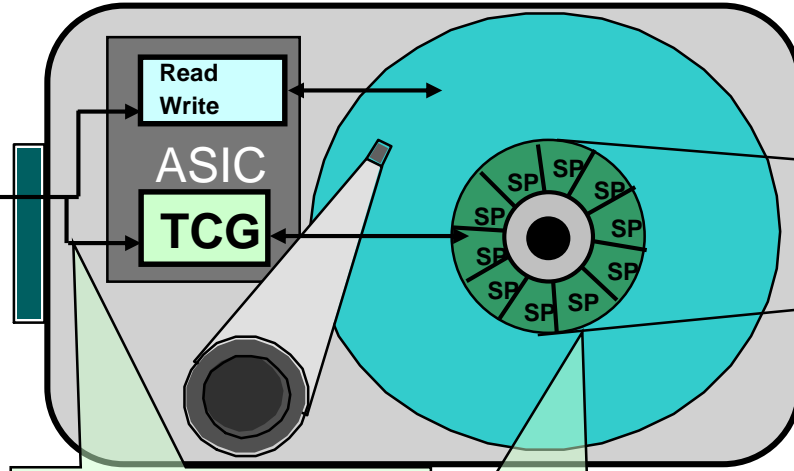
Diagnostics must be controlled

Self Encrypting Drives brought needed tools

Using standardized crypto techniques & algorithms enabled superior protection of firmware

Eventually retrofitted into all non-SED drives

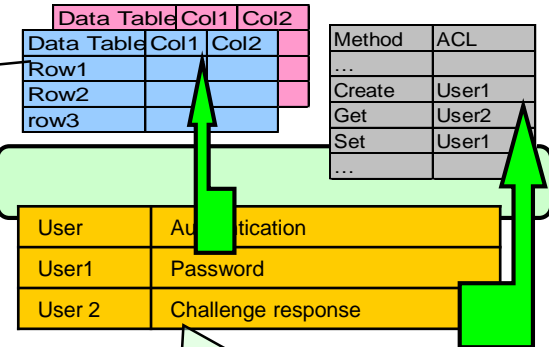
What's Inside One of These Drives:



Industry standard protocol to access security services, methods & data. Supports secure communication & strong authentication

Uncircumventable access control
Signed firmware
AES encryption in ASIC
Cryptographic methods:
AES, RSA, RNG, SHA-1, SHA-256...

High Quality RNG partly derived from media signals



Security Providers = Logical "SmartCards"
Isolated from all others & to be securely issued

Self-Encrypting Drive Basics

Locking + encryption = security

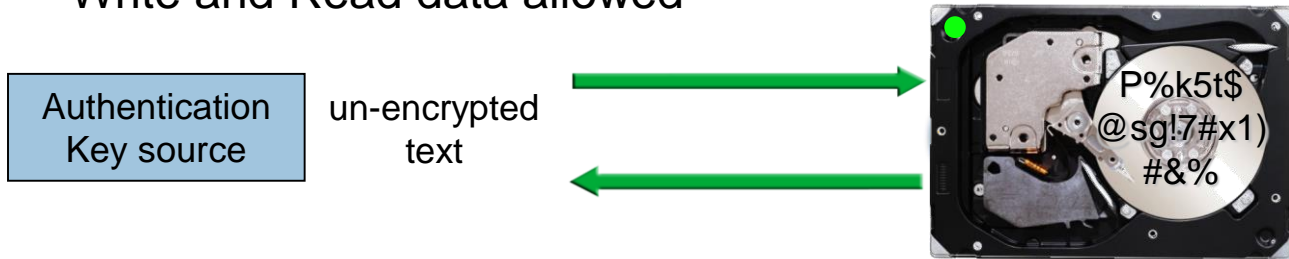
- Locking only is easily hacked (ATA has had this for years)
- Encryption only does not prevent access to data

Power OFF: SED LOCKS automatically

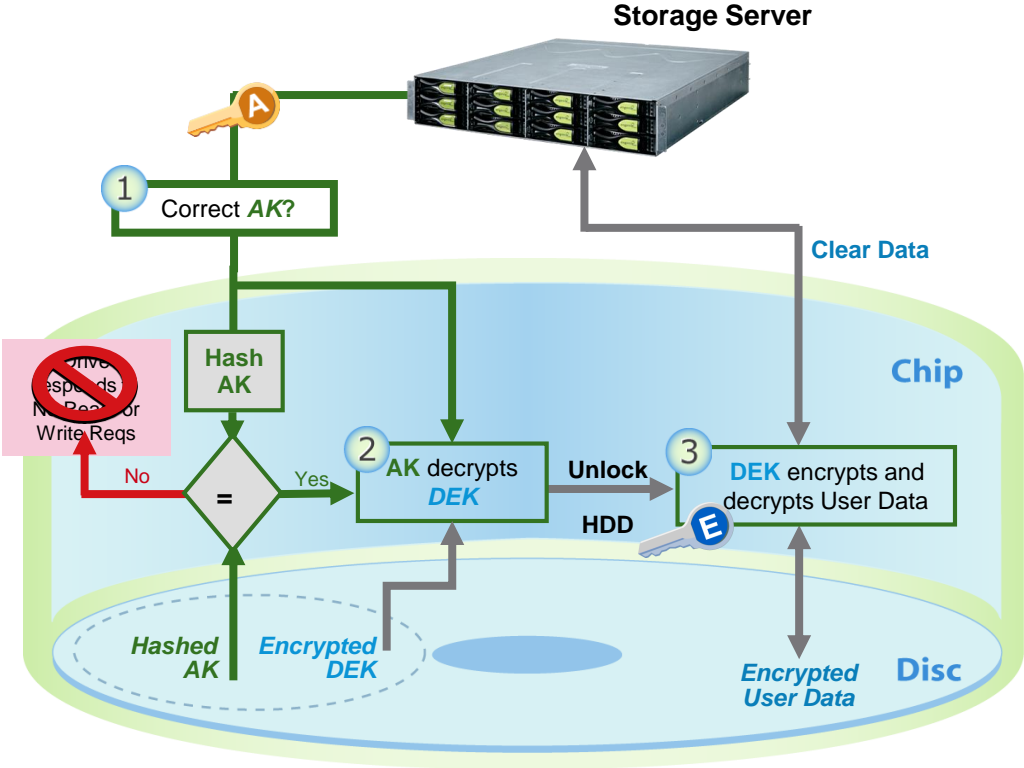
Power ON: SED remains LOCKED

Authentication Key (Password) **Unlocks** the drive

Write and Read data allowed



Authentication in the Drive



AK
Authentication Key

DEK
Data Encryption Key

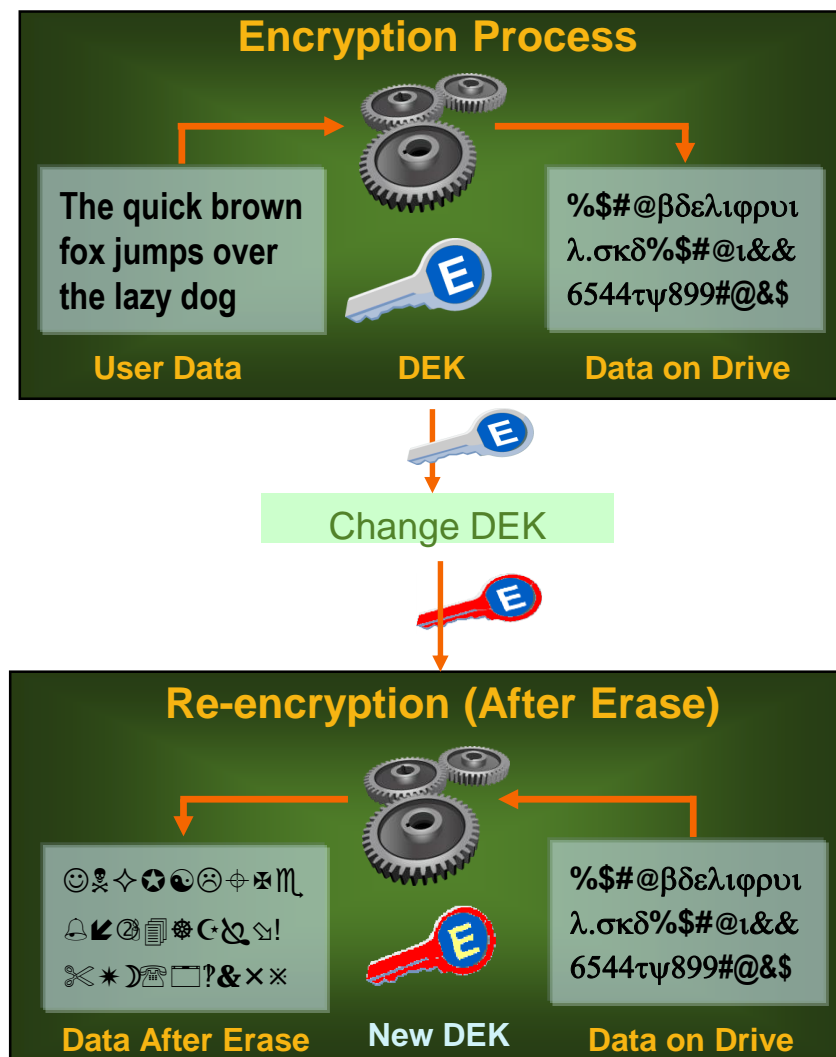
Seagate Instant Secure Erase

Description

- Instant Secure Erase changes the drive's Data Encryption Key (DEK).
- Data encrypted with previous key is unintelligible when "decrypted" with new key

Benefits

- Instantaneous erase for secure disposal or repurposing
- All spares, all virtual copies, **Everything** written with the original Key is instantly securely erased!



Media Sanitization Standards

Media Sanitization Standards: NIST SP 800-88

Public Review
Sept. 2012

Publication

NIST SP 800-88, Rev 1: Guidelines for Media Sanitization

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

- Becomes THE Federal Media Sanitization Standard
- Referenced by other Federal Standards.
- Updated with sanction and guidance for Cryptographic Erase.
- Updated with specific guidance for SSD & Hybrid Devices.

Seagate Confidential

SCSI Solid State Drives (SSDs) This includes SCSI, SAS, Fibre Channel, etc.

Clear:	Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools. The Clear pattern should be at least a single pass with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used.
Purge:	Two options are available: <ol style="list-style-type: none"> 1. Apply the SCSI sanitize command if supported. One or both of the following options may be available: <ol style="list-style-type: none"> a. The block erase command. b. If the device supports encryption, the Cryptographic Erase (also known as sanitize crypto scramble) command. Optionally: After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, the Clear procedure could alternatively be applied. 2. Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed. Refer to the TCG and vendors shipping TCG Opal or Enterprise storage devices for more information. Optionally: After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, the Clear procedure is an acceptable alternative.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.

Seagate led the industry with Media Sanitization Standards for Crypto Erase

Federal and International Standards now released

NIST 800-88 is the unified Federal Standard

Media Sanitization Standards: ISO 27040

Comments Now U.S. Vote & to ISO Sept. 2013 Publication 2013/2014

ISO / IEC 27040: Information technology-Security techniques-Storage security

<http://www.iso27001security.com/html/27040.html>

- ISO / IEC 27040 adding requirements for Media Sanitization
- Highly Leveraged from NIST 800-88
- Becomes the international standard.

Seagate Confidential

Crypto Algorithm Longevity*

Security Strength	2011 through 2013	2014 through 2030	2031 and Beyond
80	Applying	Deprecated	Disallowed
	Processing		Legacy use
112	Applying	Acceptable	Disallowed
	Processing	Acceptable	Legacy use
128	Applying/Processing	Acceptable	Acceptable
192		Acceptable	Acceptable
256		Acceptable	Acceptable

AES in any key size (128, 192, 256) is acceptable for use to 2031 and Beyond

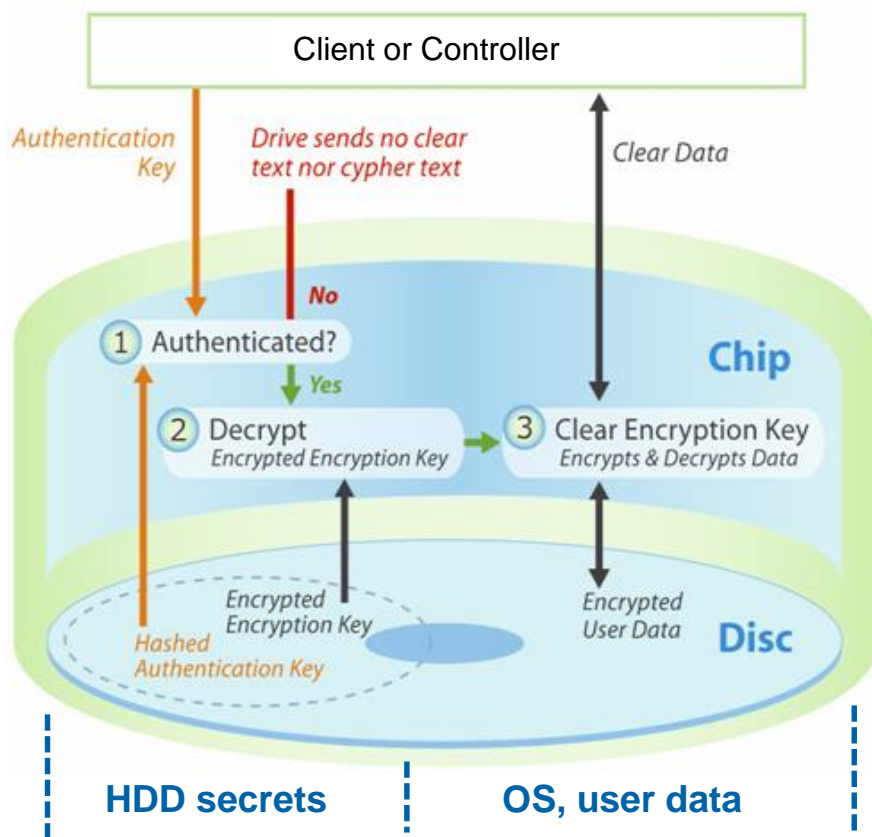
* NIST (National Institute of Standards and Technology) Special Publication 800-57
http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_geners

Seagate Confidential

ISO 27040 is the international standard.

NIST 800-57 defines algorithm longevity.

Encryption and Authentication Basics

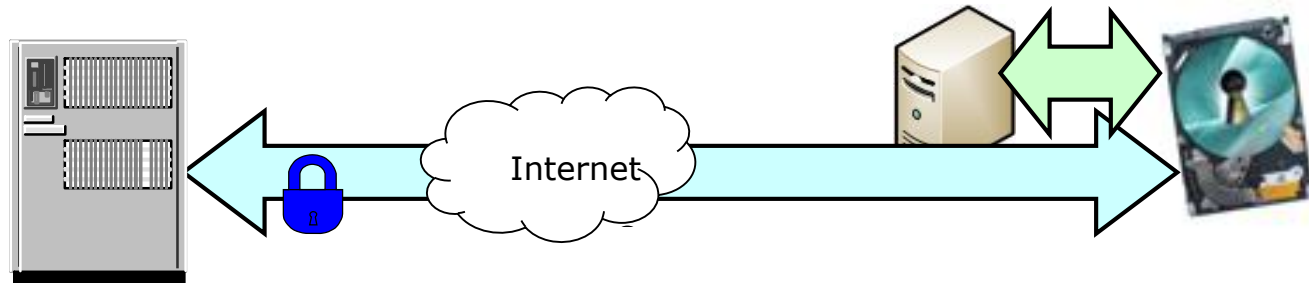


- No clear text secrets on the drive.
- Cipher text is never revealed.
- Authentication blocking after X attempts – Power Cycle required.
- Access control credentials are separated from the encryption key
- Additional credential wrap with HW Root Key.

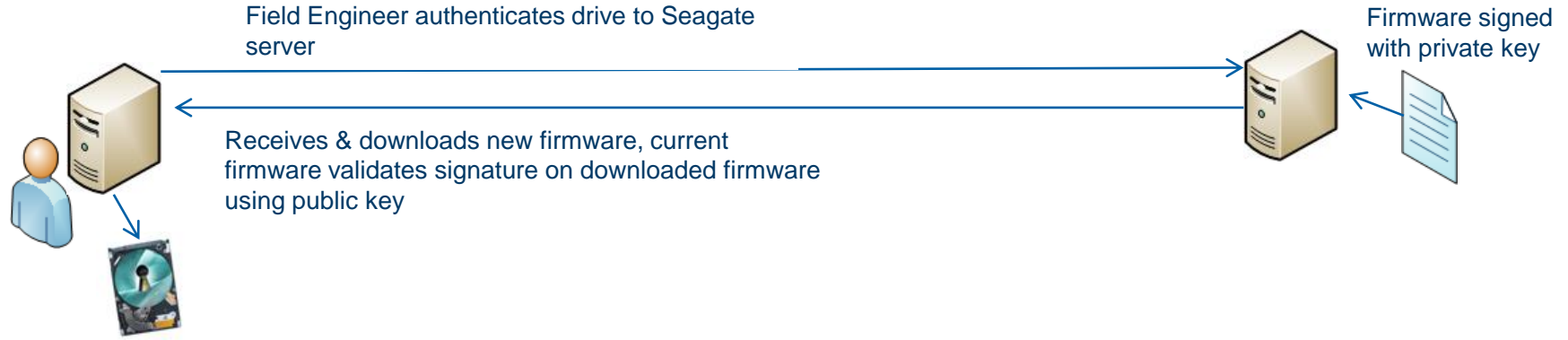
Root of Trust & Secure Communications

HDD security services can establish secure channel

- Can pass through untrusted BIOS, OS, app, WWW
- Can create session keys & secure sessions
- Can issue and respond to challenge/response sequences
- Supports PKI signing and verification
- Supports MAC & HMAC
- Has X.509 certificates for authentication



Secure Firmware Download



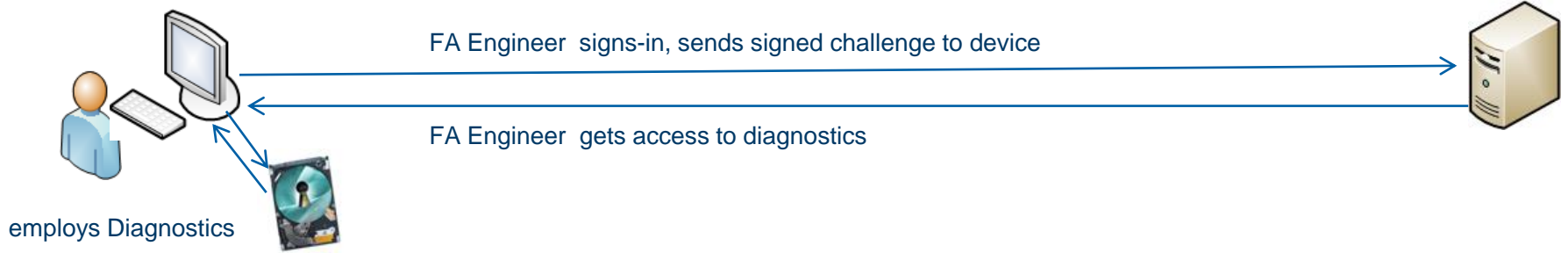
Requires cooperation of drive owner: Drive must be unlocked!

Firmware download allows only Seagate signed (using RSA2048 and SHA-256) firmware.

To load new controller firmware onto the drive, the drive verifies the integrity and authenticity of the firmware, using a replay resistant protocol exchange, before activating it.

ROM boot code verifies firmware on each power on.

Authenticated Diagnostics Command Access



Requires cooperation of drive owner: Drive must be unlocked!

Each drive is assigned an unchanging, unique security ID at manufacturing time.

Drives ship with the Diagnostic Port locked and with no Diagnostic commands. Diagnostics Port unlock via authentication through a Seagate Secure Server.

All drive protection related information is cryptographically protected on the media.

Non-repudiation log maintained for all security management activities

My Thoughts on Protecting Firmware: Key to Drive Business

You cannot outsmart the world

Secrets are eventually found out

See Brian Williams, Gary Hart, etc

Obviously NSA cannot keep a secret (Snowden)

Thinking you can is clearly no basis for intelligent action

Seagate led industry to drive encryption

Compromised firmware would threaten our leadership

Would waste millions of dollars of technical & market development

Might open the door for a competitor to leapfrog us in SED business

Our whole business depends on our firmware

If it were untrustworthy, our very existence would be threatened

Too much to risk for allowing any compromise whatsoever