SEAGATE

DRIVE SECURITY AND DATA PRESERVATION

PRESERVING DATA IN A HOSTILE ENVIRONMENT

Jon Trantham,

Principal Technologist, Seagate Technology

Designing Storage Architectures for Digital Collections 2017

Library of Congress, Washington DC, September 18th, 2017

Disclaimer

Information presented herein represents the author's personal opinion and understanding of the relevant issues involved. The author and Seagate Technology do not assume any responsibility or liability for damages arising out of any reliance on or use of this information. No warranties expressed or implied. Use at your own risk.

Key Points

- Drives with security technology are now commonplace
    - Available in most new HDD and SSD drives from major manufacturers
    - The hardware and firmware of newer drives contain anti-hacking robustness features
    - Security interface and controls are standardized across vendors
    - Drives are now available with FIPS certifications, for assurance a drive meets proven standards

- Drive security technology can be used to help digital data preservation
    - Security features can help prevent repository attacks from malware/randsomware
    - Security features now enable the creation of “WORM” drives
    - Features allow for LBA regions within a drive called bands to be protected from modification

Enemies of the Digital Data Preservationist

Storage Device Failure

- Media corrosion / oxidation, thermal decay, “Bit Rot”
- Environmental: fires, floods, earthquakes, etc.
- Latent systematic failure modes

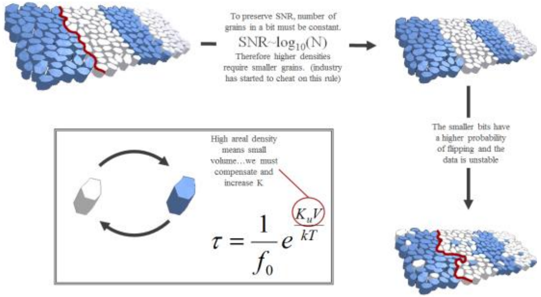
Technology Obsolescence

- Data Format Obsolescence
  - PDF 1.1, 1.2, 1.3, 1.4, 1.5…
  - BBC Domesday Project
- Interface / Protocol Obsolescence
  - SMD, ST-506, SASI, ESDI, IDE, Parallel SCSI, PATA, FCAL

Human Sources

- Accidental (accidental deletion, misplacement)
- Malicious (ransomware, hackers, disgruntled employees)
- Political (Historical Revisionism, war, budget cuts)

Security technology can help protect against human causes



To preserve SNR, number of grains in a bit must be constant.

SNR~log$_{10}$(N)

Therefore higher densities require smaller grains. (industry has started to cheat on this rule)

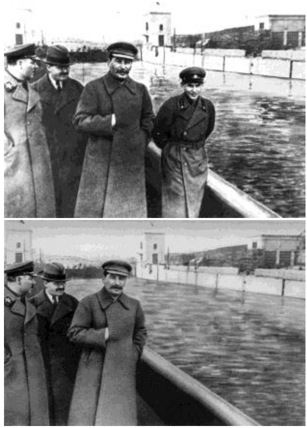
The smaller bits have a higher probability of flipping and the data is unstable

High areal density means small volume…we must compensate and increase K

$$\tau = \frac{1}{f_0} e^{\frac{K_u V}{kT}}$$

Alexandria Library Burning [2]

Domesday Project [1]



[3]

“Unpersonization” of Nikolai Yezhov

[1] By Regregex - Own work, CC BY 3.0, https://commons.wikimedia.org/w/index.php?curid=10716074
[2] Thomas Cole – The Course of Empire Destruction 1836. Public Domain
[3] Author unknown - These images are in the public domain in Russia. Refer to Licensing: https://commons.wikimedia.org/wiki/File:The_Commissar_Vanishes_2.jpg

History: ATA Security vs. TCG Opal/Enterprise

Some 1990s – 2000’s era laptops had “security” via ATA-Security protocol

- **Simple PIN-based access control mechanism**
- **Typically implemented in non-validated firmware**
- **Typically no data encryption & no provisions for secure-erase**
- **Possibly effective against common criminals, but not against real hacker adversaries**

Legislation required better data protection

- **EU Data Protection Directive (officially Directive 95/46/EC) - 1995**
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA) – 1996 – personal information privacy**
- **California Security Breach Information Act (CA SB 1386) – 2002 – required encryption**
- **Public Company Accounting Reform and Investor Protection Act (Sarbanes-Oxley / SOX 404) – 2002 – IT controls**

In response, data storage industry formed standards for drive encryption technology

- **Partnered with the *Trusted Computing Group* and ANSI-T10/T13 to form security specifications for drives**
  - TCG Opal for Laptop / Notebook / Desktop drives and TCG Enterprise for Enterprise server drives
- **US Government formed standards under NIST for data encryption, key management, tampering, secure erasure…**

The result was more secure, standardized products for data loss prevention

Hardening of HDDs & SSD Designs

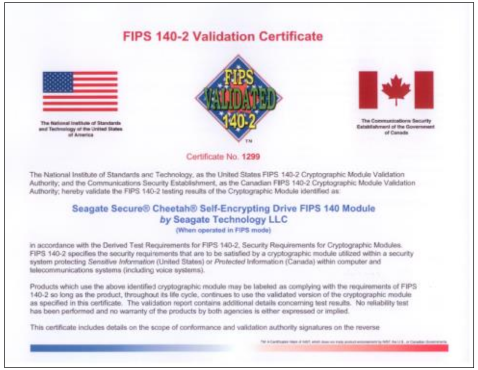
1. **Secure-Boot**
   - Cryptographically Signed & Validated Drive Firmware
   - ROM in storage device loads firmware from flash and validates it with public key
   - Rogue firmware detection

2. **Security hardware - common in most (if not all) new drive controllers**
   - AES256-XTS, SHA engines, random number generators, RSA PKCS, etc.

3. **Secure-Diagnostics: Locked Debug Ports**
   - Vendor-unique commands and debug features cryptographically locked down
   - Hardware debug ports, such as JTAG and manufacturing serial ports locked down

4. **FIPS 140-2 / FIPS 140-Next / Common Criteria Security**
   - Federal Info Processing Std. 140 Certifications, Anti-Tampering Features

5. **US Federal Trade Agreements Act “TAA” Compliance (19 USC 2501-2581)**
   - Known Provenance, Trusted Life Cycle, Device Root of Trust, Secure Supply Chain
   - Required in many governmental data storage applications



FIPS 140-2 Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

FIPS
VALIDATED
140-2
TM

Certificate No. 1299

The National Institute of Standards anc Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

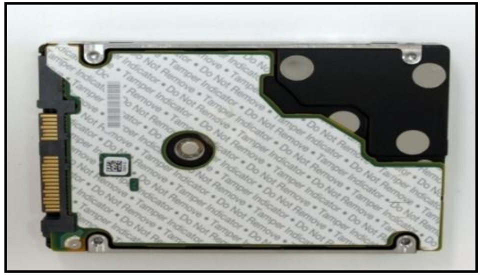
Seagate Secure® Cheetah® Self-Encrypting Drive FIPS 140 Module
by Seagate Technology LLC
(When operated in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

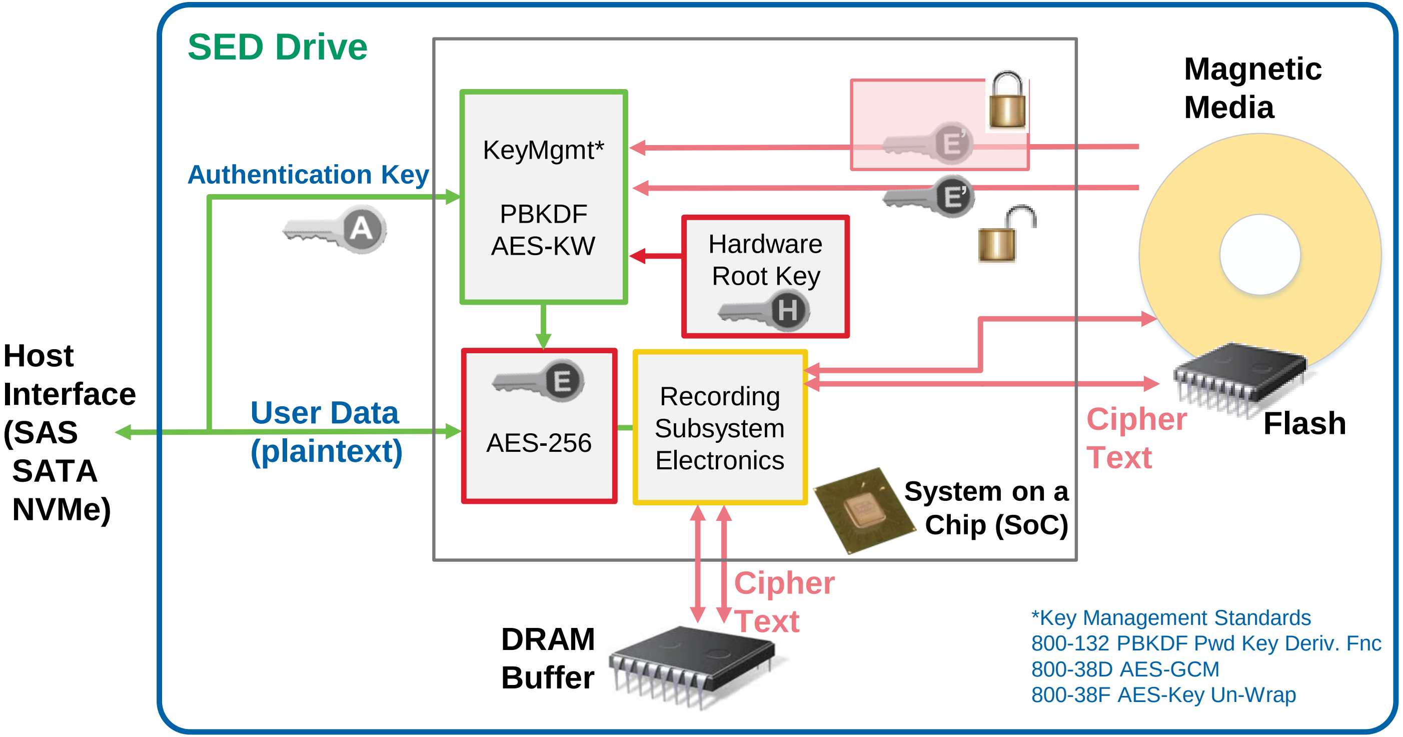
This certificate includes details on the scope of conformance and validation authority signatures on the reverse

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments



Protecting User Data – Seagate Encryption Design Aspects

All user data are encrypted in DRAM, Flash, Magnetic Media with AES-256



*Key Management Standards
800-132 PBKDF Pwd Key Deriv. Fnc
800-38D AES-GCM
800-38F AES-Key Un-Wrap

Important Design Aspects

- User data are encrypted upon receipt
  - with AES-256-XTS
- User data are encrypted in-buffer
  - Prevents frozen DRAM attacks
- Unwrapped Encryption Key E exists only internally within SoC registers
  - Encryption key on media (E') is always wrapped with Hardware's Root Key (H) – This key is unique & private to each controller chip
  - Encryption key on media (E') may be further wrapped with user's Authentication key (depends upon drive type and settings)
  - Key changes, such as during Instant secure erase, generate a new encryption key (E)

Commonly Available Security Features

On most new drives:

1. **Device Data Destruction - "Instant Secure Erase" (ISE)**
   - Drive data are erased cryptographically in seconds via key destruction
   - Typically used when drives are re-purposed or destroyed
   - Standardized via NIST 800-88, NIST 800-57, ISO 27040

Features generally available on FIPs140-2 and TCG-compliant drives:

2. **Encryption – "Data at Rest" Security**
   - User data on the storage device is not accessible without authentication

3. **Band Locking –**
   - Logical Bands of LBA's can be set to require authentication to access
   - Logical Bands (including entire drive) can be made Read-Only / Write-Only
     - Read-only capability - important for data preservation
     - Write-only capability - for security of field video surveillance, logging applications
   - For preservation, data can be written to the drive and then the storage band can be set read-only
     - Data in a read-only band can be set up to readable without authentication
     - Data stored in a read-only band cannot be altered or erased without authentication

4. **Port Locking – Enable/Disable features is under access control**
   - For example, firmware download can be disabled

Advice for the Data Preservationist

Or more specifically, for your supporting IT personnel:

1. **Be aware of the type of drives offered and their features**
   - Whether it contains TCG security features, FIPs 140 certifications, instant secure erase, secure code validation, etc.
   - Be aware of command behavior under command set.
     - For example, a FIPS drive shuts off open T-10 sanitize in FIPS mode and controls erasure via authentication, whereas a SED drive may not.

2. **Take ownership control of your drive's security**
   - Drive are shipped with default credentials (keys), set to MSID (manufacturer's SID).
   - MSID can be queried through the drive's interface and changed to something secret
     - You (the owner) want to do this and not leave it open for a hacker to do so
     - This must be done for all resource authorities (e.g. the administration SP, the BandMaster, the EraseMaster, etc.)
   - This typically done with a replicated key server

3. **Learn the various security features options of your drives and set them accordingly**
   - For example, enabling the *Instant Secure Erase* feature may be undesirable for drives storing public information
   - On the other hand, ISE may be very important for drives storing confidential information
   - ISE behavior can vary between drive type.

4. **Consider changing security settings over the drives life as your needs change**
   - For example, by setting data bands to read-only if data will no longer be updated

5. **Test and validate any security-related software on small samples before wider deployment**
   - To reduce the chances of widespread data loss through human error

Summary

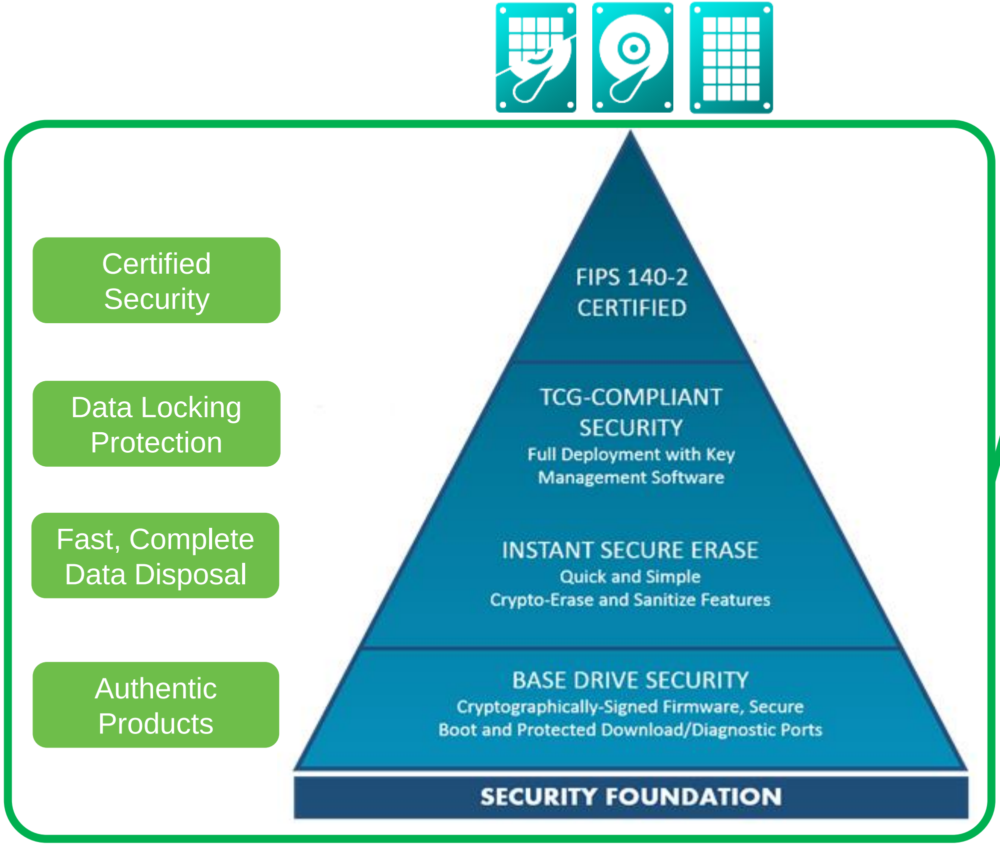
- Data storage devices (drives) are always targets for hackers and thieves
- Drive security features have evolved to counteract these threats
- Security technology is now commonplace in most new drives
- FIPs certified drives provide the buyer assurance a drive meets standards
- Drive security technology can be used to help digital data preservation

Additional Reference Information

Further Reading

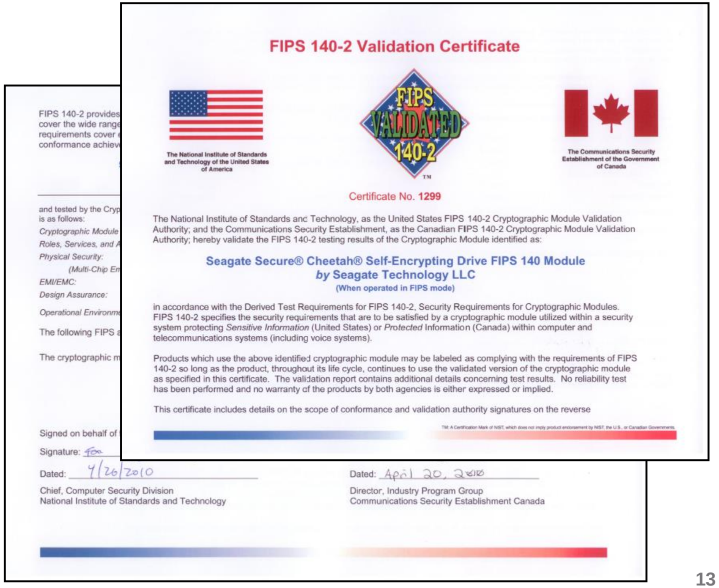
1. http://www.seagate.com/files/staticfiles/support/docs/manual/Interface%20manuals/100515636b.pdf
2. https://trustedcomputinggroup.org/work-groups/storage/
3. https://www.trustedcomputinggroup.org/wp-content/uploads/SWG_TCG_Enterprise-Introduction_Sept2010.pdf
4. https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage_Enterprise_SSC_App_Note_v1_r1_Final.pdf
5. https://trustedcomputinggroup.org/wp-content/uploads/Architects-Guide-Data-Security-Using-TCG-Self-Encrypting-Drive-Technology.pdf
6. http://www.snia.org/sites/default/education/tutorials/2012/spring/security/MichaelWillett_Implementing%20Stored-Data_Encryption_2.pdf

Transparent and Certified Security (FIPS)



Certified Security
Data Locking Protection
Fast, Complete Data Disposal
Authentic Products
FIPS 140-2 CERTIFIED
TCG-COMPLIANT SECURITY
Full Deployment with Key Management Software
INSTANT SECURE ERASE
Quick and Simple Crypto-Erase and Sanitize Features
BASE DRIVE SECURITY
Cryptographically-Signed Firmware, Secure Boot and Protected Download/Diagnostic Ports
SECURITY FOUNDATION

FIPS 140-2 validation provides certified assurance that a device's cryptography technology meets NIST standards required for sensitive data storage, covering areas such as security, protection profiles, random number generation, key establishment, and tamper resistance.



FIPS 140-2 provides
cover the wide range
requirements cover
conformance achiev

and tested by the Cryp
is as follows:

Cryptographic Module

Roles, Services, and A

Physical Security:

(Multi-Chip Em

EMI/EMC:

Design Assurance:

Operational Environme

The following FIPS a

The cryptographic m

Signed on behalf of

Signature:

Dated: 4/26/2010

Chief, Computer Security Division
National Institute of Standards and Technology

Dated: April 20, 2010

Director, Industry Program Group
Communications Security Establishment Canada

FIPS 140-2 Validation Certificate

The National Institute of Standards and Technology of the United States of America

FIPS VALIDATED 140-2 TM

The Communications Security Establishment of the Government of Canada

Certificate No. **1299**

The National Institute of Standards anc Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

Seagate Secure® Cheetah® Self-Encrypting Drive FIPS 140 Module
***by* Seagate Technology LLC**
(When operated in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected* Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments.

FIPS 140-2 Security Levels

Level 1

- Requires a cryptographic module, no physical security

Level 2

- In addition to a cryptographic module, requires to show evidence of tampering with physical security

Level 3

- Adds prevention of access critical security parameters held within the cryptographic module and may include mechanisms may include the use of strong enclosures and tamper-detection/response circuitry that zeroes all plaintext

Level 4

- Adds physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access

Trade Agreements Act

- The Federal Trade Agreements Act (19 U.S.C 2501-2581) is also Known as “TAA” of 1979 was enacted to foster fair and open international trade, but more importantly, it implemented the requirement that the U.S. Government may acquire only U.S.-made or -designated end products
  - The cost of its components mined, produced, or manufactured in the U.S. exceeds 50 percent of the cost of all of its components
  - Products must undergo “substantial transformation” within the US or TAA country
- US Government procurement requires TAA for many projects
  - GSA contracts – regardless of cost (min thresholds do not apply)
  - DOD contracts
  - IDIQ (indefinite delivery, indefinite quantity) contracts

Seagate Product TAA Compliance

Seagate has certified methods for Trade Agreements Act (TAA) compliance in USA, Singapore, South Korea

U.S. Customs and
Border Protection

Seagate Certified for Designed in USA

Enterprise, Mission Critical & Desktop

The Customs and Border Protection (CBP) issued a final determination on August 15,2013 that certain Seagate HDDs, including SED HDDs, are substantially transformed in the U.S. and **for purposes of U.S. Government procurement are products of the United States.**

Ruling specifics:

- Drives in the following market segments:
  Business Critical, Mission Critical, Desktop
- Includes 80% of USA-based R&D Content with firmware programmed in the US and of US origin
- Follows a process where HDDs arrive into USA as non-functional with no active firmware

Excludes: Client Notebook Hard Drives

The Customs and Border Protection (CBP) issued a final determination on November 30, 2016 that for hard disk drives where "the firmware for the hard disk drives is primarily written and installed … in the same country", **for purposes of U.S. Government procurement are products of either Singapore or South Korea.**

Ruling specifics:

- Drives in the following market segments: Notebook
- Includes 80% of Singapore/South Korea-based R&D Content with firmware programmed in the Singapore/South Korea and of Singapore/South Korea origin
- Follows a process where HDDs arrive into Singapore/South Korea as non-functional with no active firmware