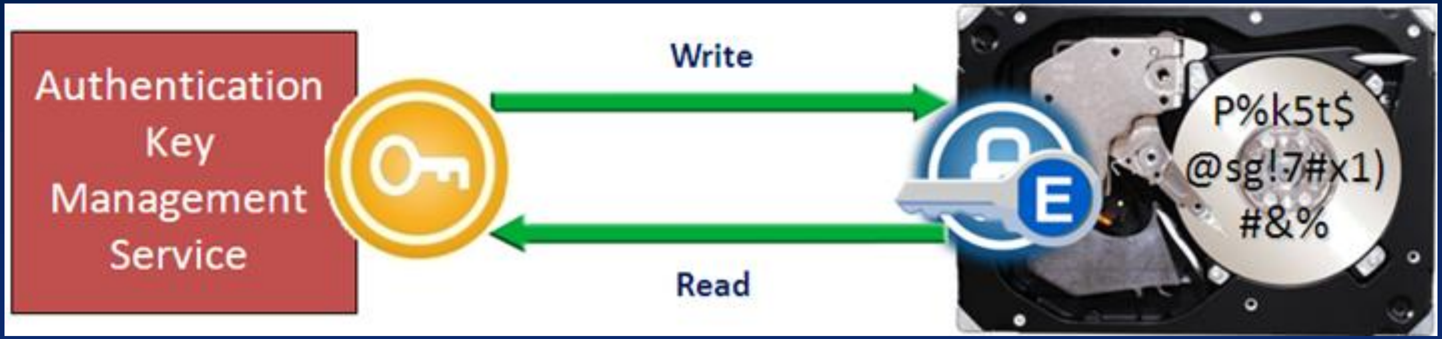
Self Encrypting Drives: SSD, SSHD, Enterprise and Opal and FIPS”

Session 103-A: Security

Monty A. Forehand

Seagate Technology

Self-Encrypting Drives (SEDs)



- Hardware Encryption – All the bits, all the time, at-speed.
- Embedded Security and Encryption key generation/management
- Standard Security Interfaces - Locking, Band, & Access Mgmt.

- Consumer Gets:
  - Superior performance to Software/Host based FDE.
  - Strong Data at Rest Protection – Auto Lock on Power-off.
  - Strong Instant Secure Erase.
  - No need for re-encryption on deployment and upgrades.

Good Security

- Consumers need assurance of Good Security:
  - Some vendors have FIPS 140 Certified SED in multi-generation production.
  - More Vendors FIPS 197 AES certified SED in multi-generation production.
  - Eminent Draft Standard for Cryptographic Erase best practices from NIST.

Standards

- **TCG Enterprise SSC :** Security Mgmt. for Server / Cloud systems.
    - Version 1 devices in-production for Multiple Generations.
- **TCG Opal SSC** – Security Mgmt. for Client systems.
    - Version 1 devices in production for multiple Generations.
    - Version 2 devices in the market this year.
    - Single User Mode & Data Store Table Feature Sets : Enabling native Win8 SED support

- **T10 / T13 (NCITS)**
    - Support for TCG Trusted Send/Receive Commands – Shipping multiple generations.
    - Recently Added Sanitize Feature set (Crypto Erase, Block Erase, Overwrite).

- **IEEE-1667 : TCG Storage Silo**
    - Enabling Win8 eDrive = native SED support in Windows / Windows Server
    - Devices in the market this year.

- **UEFI 2.3.1 :** Native support for TCG SED Commands
    - Enabling secure system boot using UEFI & SED.

- **NIST SP 800-88** : Data Sanitization Requirements
    - Industry consortium with NSA & NIST to achieve Cryptographic Erase standards.
    - Eminent update expected detailing Cryptographic Erase Requirements.

SED for SSHD and SSD

- All of the goodness of SED applies to SSHD and SSD.
- Software / Host FDE performance reduced as much as 2/3 *1
  - No performance penalty for SED on SSHD / SSD.
- Encryption is required to reach expired silicon storage locations for erasure. *2
  - OPEN Session 104-A: What, Me Worry? Is Flash Secure Today? (Security Track). Immediately following (3:30 pm).
- Self-Encrypting SSDs in the market today, and SSHD coming soon .

*1 http://anthonyvance.com/blog/security/ssd_encryption/

•*2 Coughlin, 2011 Self Encrypting Drive Market and Technology Report

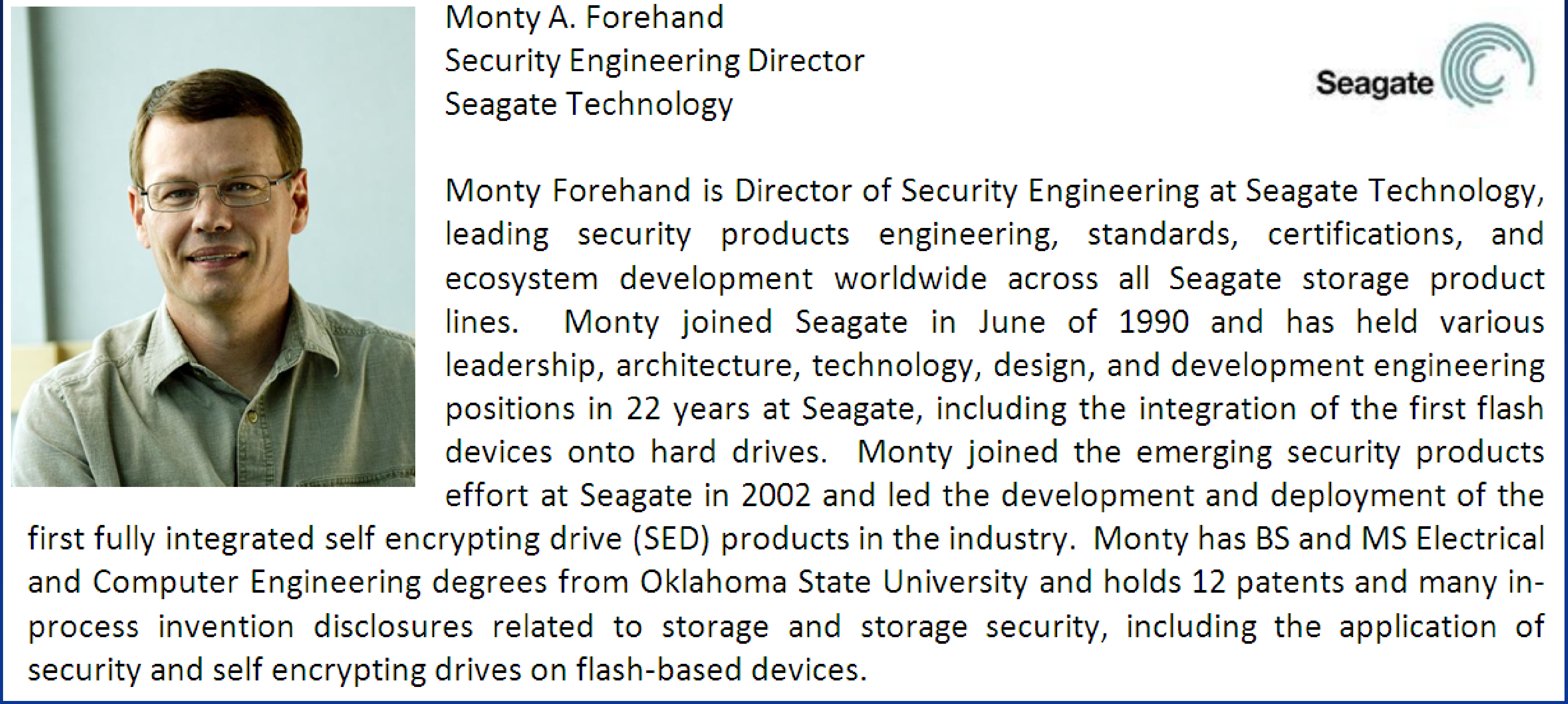
SSD = Solid State Drive
SSHD = Solid State Hybrid Drive
SED = Self Encrypting Drive

Calls to Action

- Continue Momentum on Enterprise SSC Devices.
- Deploy Opal 2 & eDrive Devices, Systems, & Management Software.
- NIST SP 800-88 update release and ratification of Cryptographic Erase.
- Encryption on all SSHD and SSD.
- More SED devices, systems, & management software.

Back-up

Speaker Bio



Monty A. Forehand
Security Engineering Director
Seagate Technology

Seagate

Monty Forehand is Director of Security Engineering at Seagate Technology, leading security products engineering, standards, certifications, and ecosystem development worldwide across all Seagate storage product lines. Monty joined Seagate in June of 1990 and has held various leadership, architecture, technology, design, and development engineering positions in 22 years at Seagate, including the integration of the first flash devices onto hard drives. Monty joined the emerging security products effort at Seagate in 2002 and led the development and deployment of the first fully integrated self encrypting drive (SED) products in the industry. Monty has BS and MS Electrical and Computer Engineering degrees from Oklahoma State University and holds 12 patents and many in-process invention disclosures related to storage and storage security, including the application of security and self encrypting drives on flash-based devices.