Solid State Drives (SSD) with Self Encryption: Solidly Secure

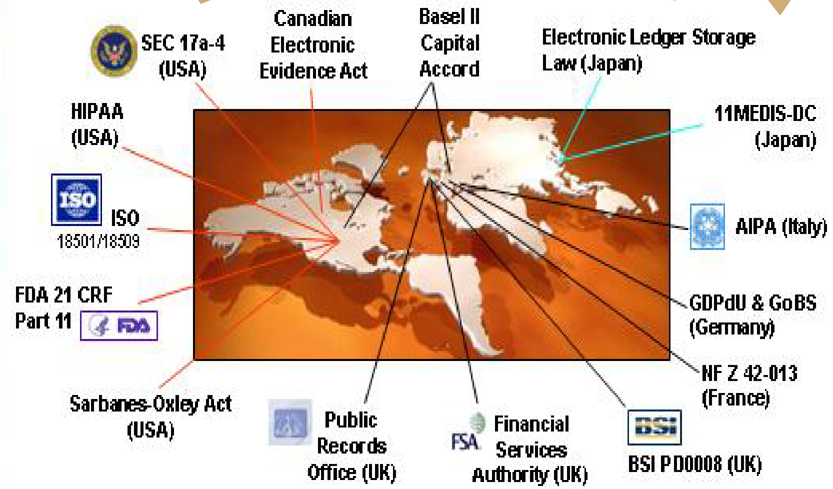
Michael Willett
Storage Security Strategist
Independent Consultant

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



tp://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

ge cost of $5.4
er record

$5.4 Million Per Incident

Financial

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

Reputation

tp://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"

Trusted Storage Standardization

TRUSTED COMPUTING GROUP™

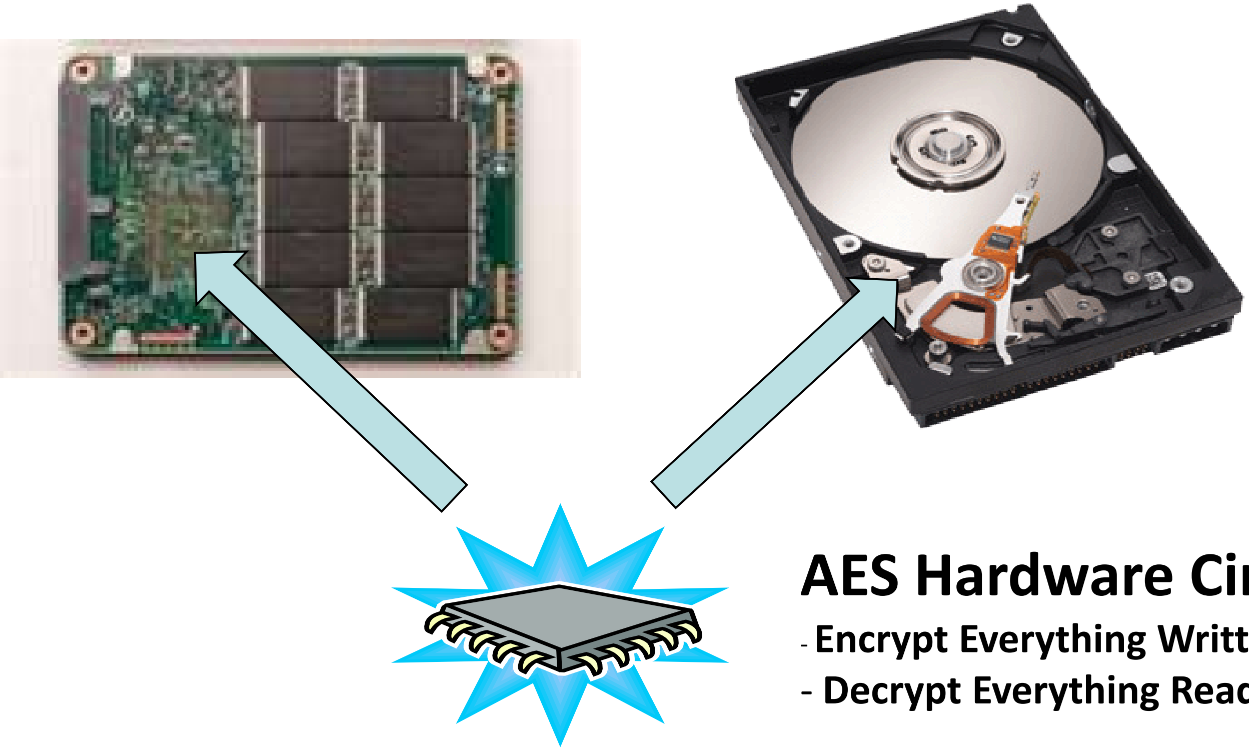
Published Storage Specifications

Self-Encrypting Drives (SED)

What is a Self-Encrypting Drive (SED)?

Trusted Computing Group
SED Management Interface

Interface



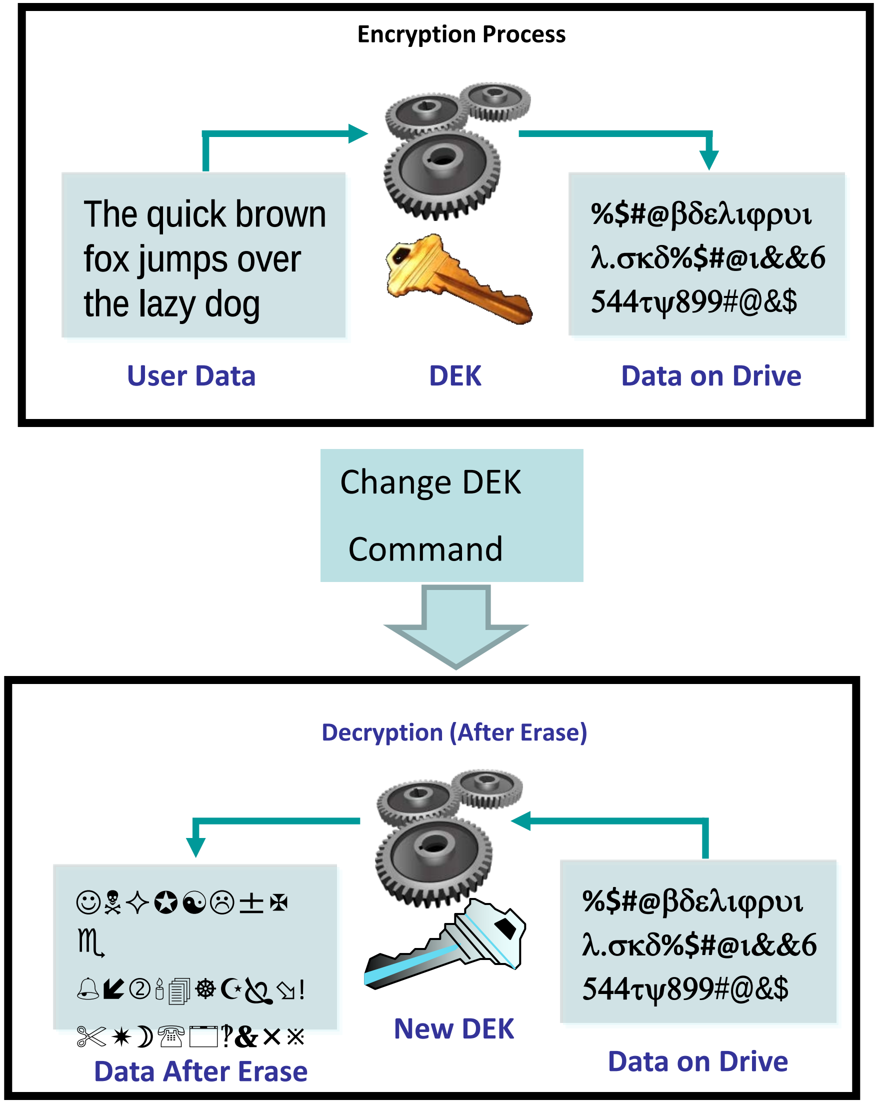
AES Hardware Circuitry

- Encrypt Everything Written
- Decrypt Everything Read

Crypto 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
- 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



Encryption Process

The quick brown fox jumps over the lazy dog

%$#@βδελιφρυι λ.σκδ%$#@ι&&6 544τψ899#@&$

User Data

DEK

Data on Drive

Change DEK Command

Decryption (After Erase)

☺☠✧✪☯☹±✠
♏
🔔⬋②🕯🗐☸☪🙮⬂!
✂✷☽☎🗔⁈&✕※

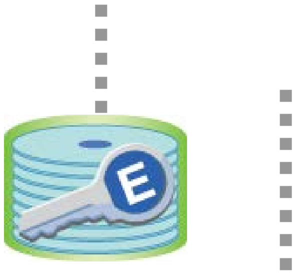
Data After Erase

New DEK

%$#@βδελιφρυι λ.σκδ%$#@ι&&6 544τψ899#@&$

Data on Drive

No Performance Degradation



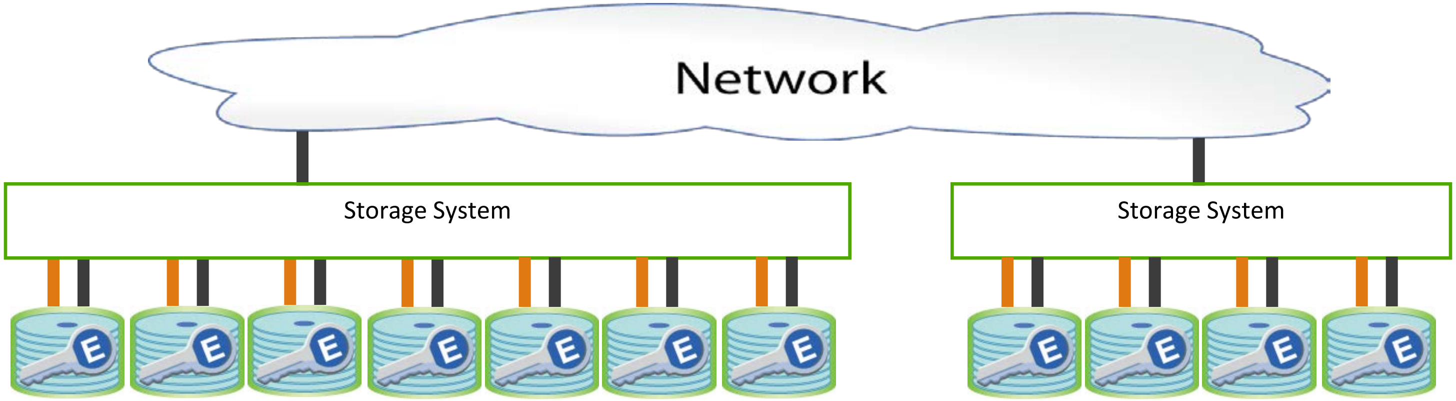
Encryption engine speed

<u>Matches</u>

Port’s max speed

The encryption engine is in the drive electronics

Scales Linearly, Automatically



Network

Storage System

Storage System

All data will be encrypted, with no performance degradation

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

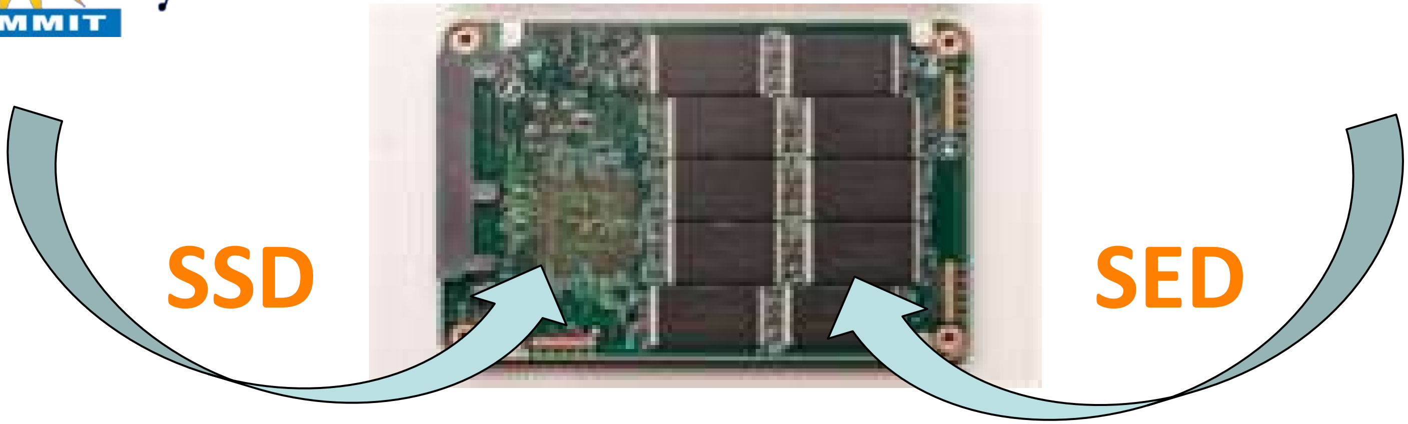
MB/Sec	HDD: no encryption	HDD: S/W encryption	HDD: SED	SSD: no encryption	SSD: S/W encryption	SSD: SED
Startup	7.90	6.97	7.99	82.50	47.90	95.33
App Loading	7.03	5.77	5.71	48.33	30.77	60.37
Modest size file test	6.13	5.00	5.28	41.13	26.77	50.40
Large Scale Data Read	84.67	52.88	82.75	178.00	70.23	169.33
Large Scale Data Write	79.60	49.50	50.31	170.80	63.60	164.50

http://www.trustedstrategies.com/

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

Solid-State Drive + Self-Encrypting Drive



SIMPLE SOLUTION

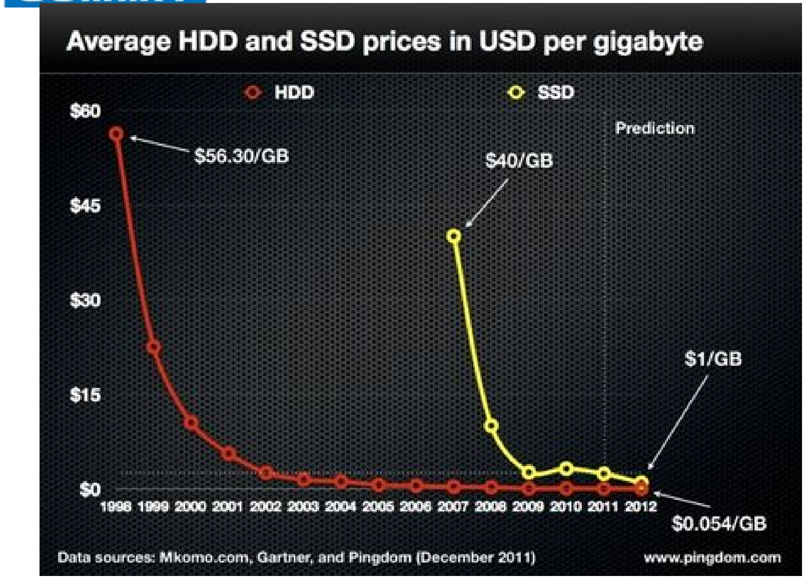
- Reduced TCO
- Increased productivity
- Better Performance
- More shock resistance
- Better reliability
- Less power use
- Approaching price parity re: HDD

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

- Scalable
- Interoperable
- Integrated
- Transparent

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 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/

Saint Barnabas Health Care System: SED 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

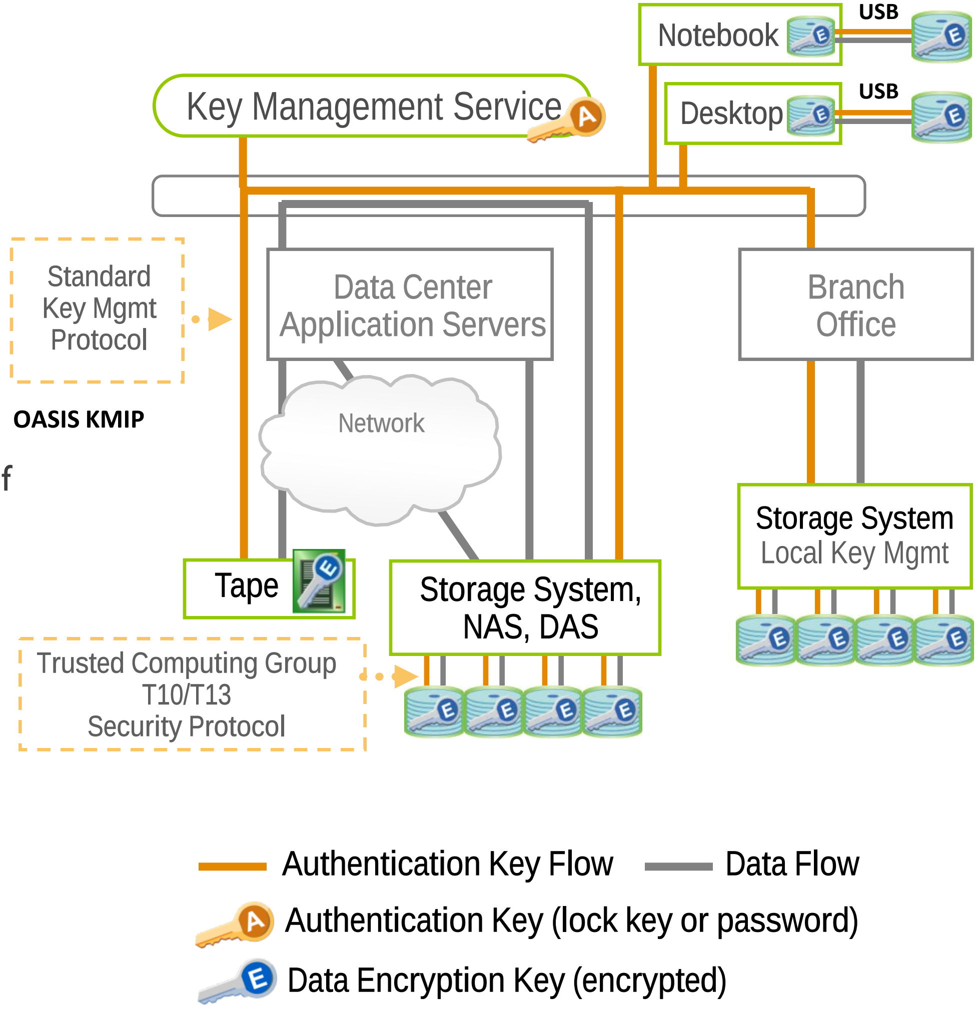
BARNABAS HEALTH

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
- 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

The Future: 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



Key Management Service

Notebook

USB

Desktop

USB

Standard Key Mgmt Protocol

OASIS KMIP

Data Center Application Servers

Network

Branch Office

Storage System Local Key Mgmt

Tape

Storage System, NAS, DAS

Trusted Computing Group T10/T13 Security Protocol

Authentication Key Flow — Data Flow

A Authentication Key (lock key or password)

E Data Encryption Key (encrypted)

Thank You!