



# Encryption Key Management Simplified

**Townsend Security**



## Presenter: Liz Townsend

- Director of Business Development Townsend Security
- Regularly speaks at industry events and conferences
- Produced seven eBooks on encryption and key management

### Contact Liz Townsend

[liz.townsend@townsendsecurity.com](mailto:liz.townsend@townsendsecurity.com)



## Introduction

- What is encryption key management and why is it important?
- Addressing perceived risks of encryption key management
- Critical components of a professional key manager
- What you will take away from this session
  - Encryption key management basics
  - Overcoming key management challenges

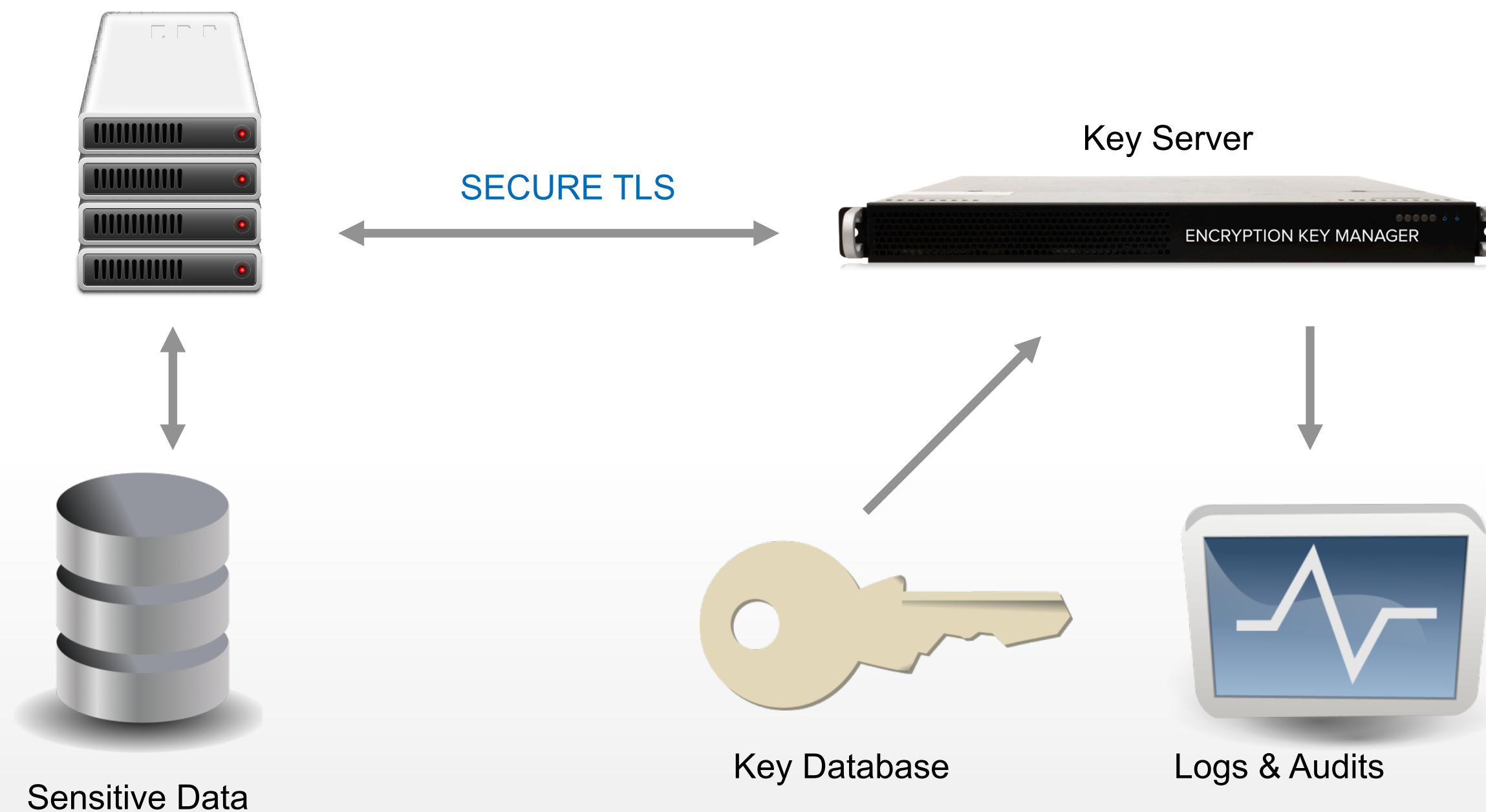


## What is Encryption Key Management?

- Protects the keys to your kingdom
- Critical part of an encryption strategy
- Cryptographic module in hardware (HSM), virtual, or the cloud
- Creates, stores, manages, protects encryption keys

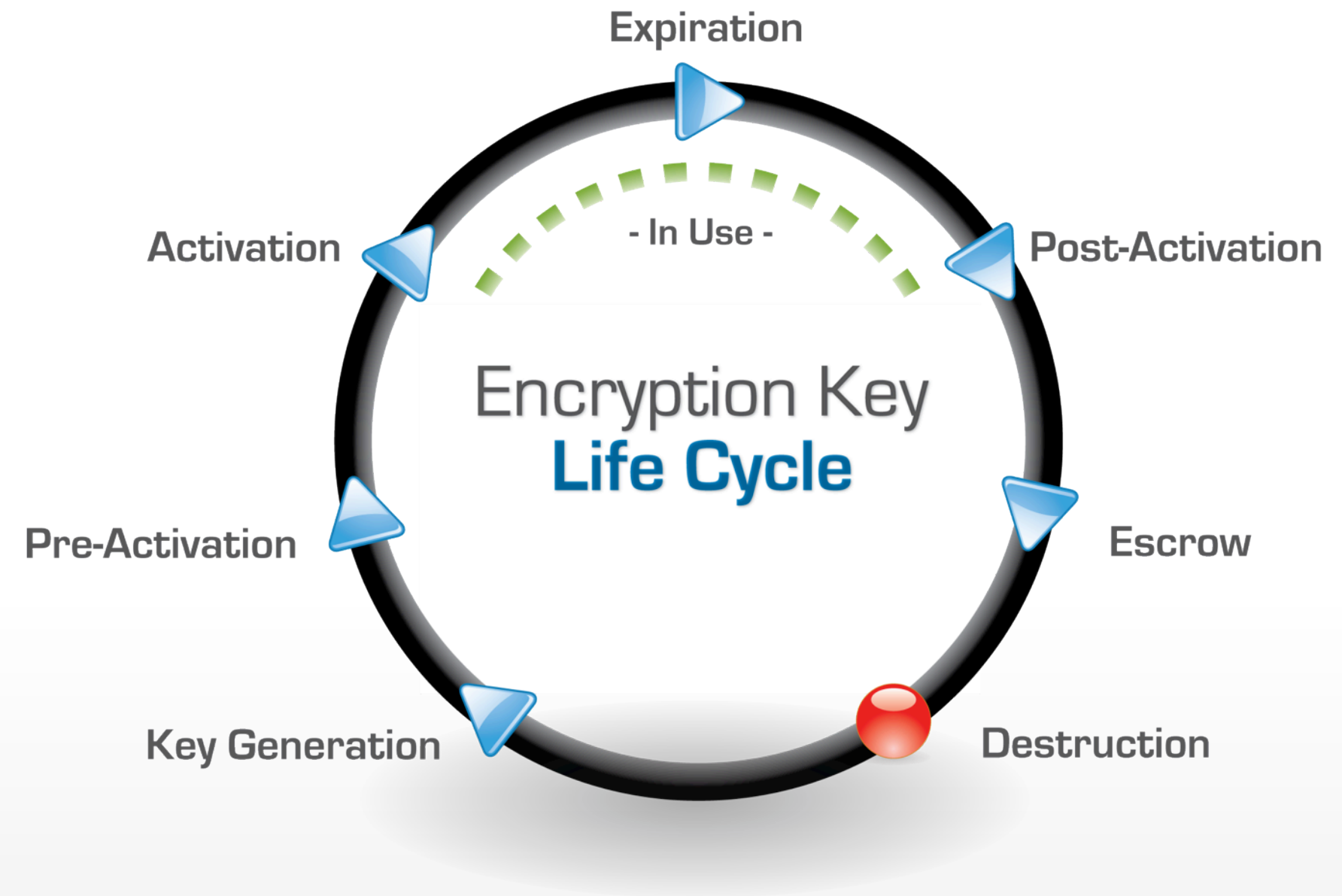


# Key Management Server & Key Retrieval



## Encryption Key Life Cycle

- Create strong encryption keys
- Activate, expire, compromised, revoke, backup, destroy
- NIST describes the life cycle of keys



## Components of an Encryption Key Manager

Key Life Cycle Management

Key Mirroring

Key Creation – DEKs, KEKs

Distributing Keys

Securely Storing Keys

Access Control

Defining Key Attributes

Systems Management & Audit

High Availability

Certifications

Backup and Restore

Admin Management



## Why is key management important?

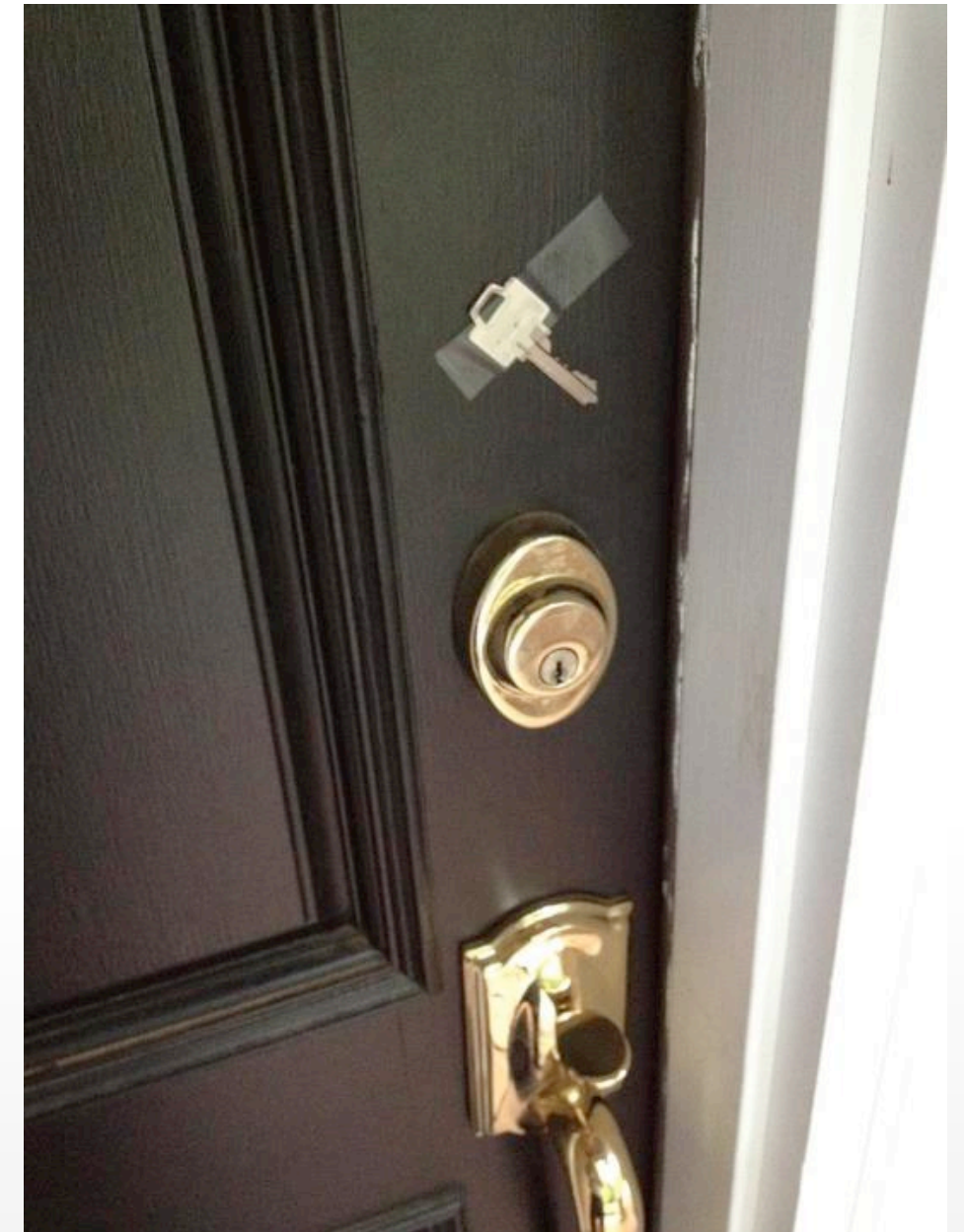
- Preventing a data breach (encryption is only half the solution!)
- Meeting compliance regulations



## Don't Do This



- Hackers don't break encryption, they find the keys
- History lessons learned from tapes drives falling off backs of trucks.



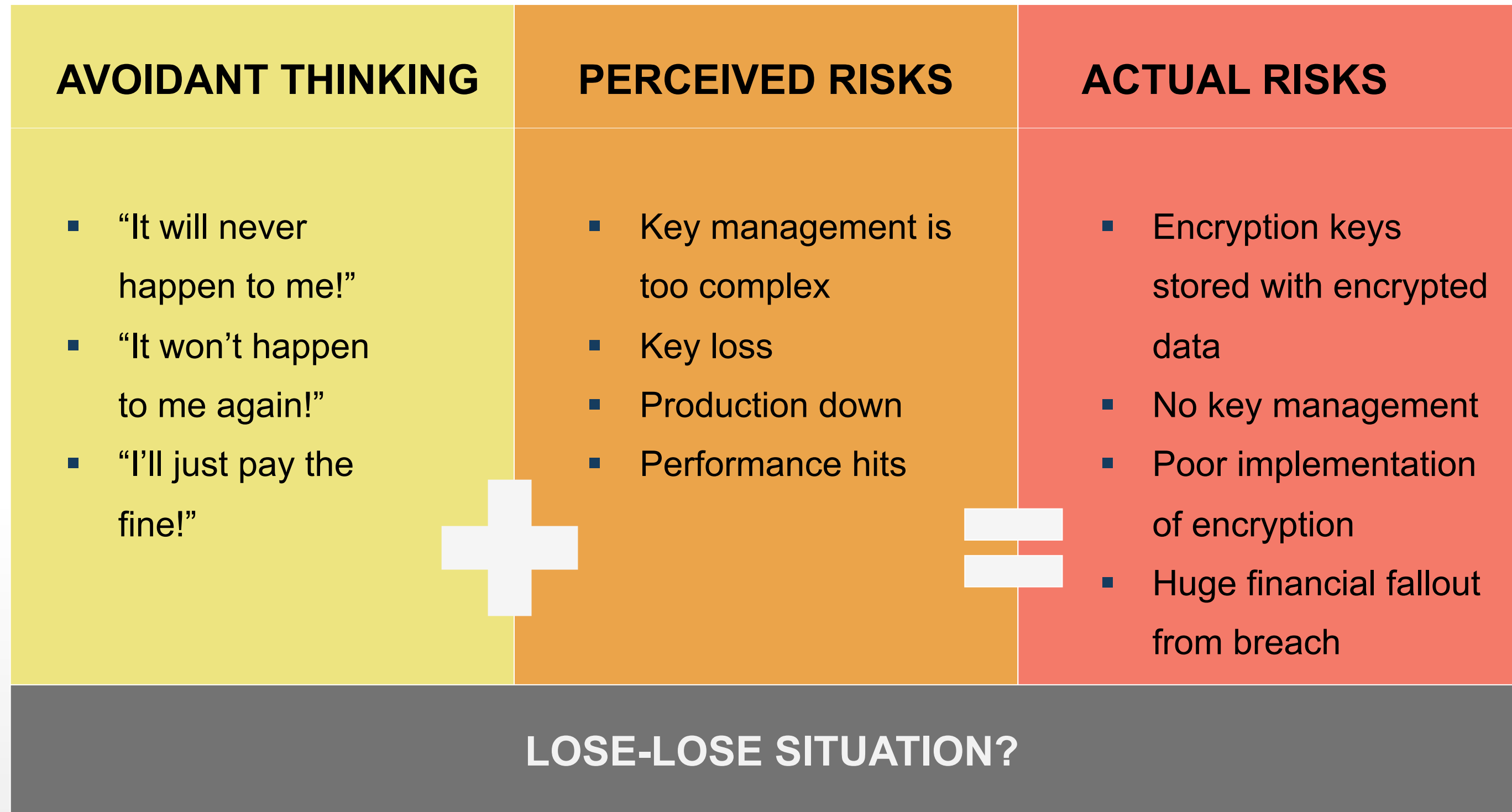
## Meeting Compliance with Key Management

- PCI, HIPAA, FFIEC, SOX, etc. reference NIST standards for key management
- Reference NIST for key management best practices (SP 800-57)
- Don't always require key management, difficult to meet compliance without key management
- Meeting compliance is difficult using homegrown or DIY solutions
- Meeting compliance can be a low bar



## Why is Key Management Difficult to Implement?

- Key management has a reputation for being risky and costly
- Avoidant thinking by business leaders
- Perceived risks stop a key management project in its tracks





**LOSE-LOSE SITUATION?**

**AVOIDANT THINKING**

- “It will never happen to me!”
- “It won’t happen to me again!”
- “I’ll just pay the fine!”

## What We Know About Data Breaches Today

- “When” not “if”
- Hacking is a multi-billion dollar business
- Cost of data breach includes much, much more than the fine
- Cost includes fines, litigation, costs from banks, credit monitoring, brand damage, customer loss
- Data breach often seen as “poor governance and risk management”

## PERCEIVED RISKS

- Key management is too complex
- Key loss
- Production down
- Performance hits

## Professional Key Management *Mitigates* These Risks

- Key management *everywhere* your data is
- Key management built on RESTful APIs
- Audit logs of all key management activity
- SIEM integration for best security
- High availability & business continuity
- KMIP
- Certifications
- Robust support from vendor

# **Enterprise Key Management Should Address and Solve All Risks**

## **What to Look For in an Enterprise Key Manager**

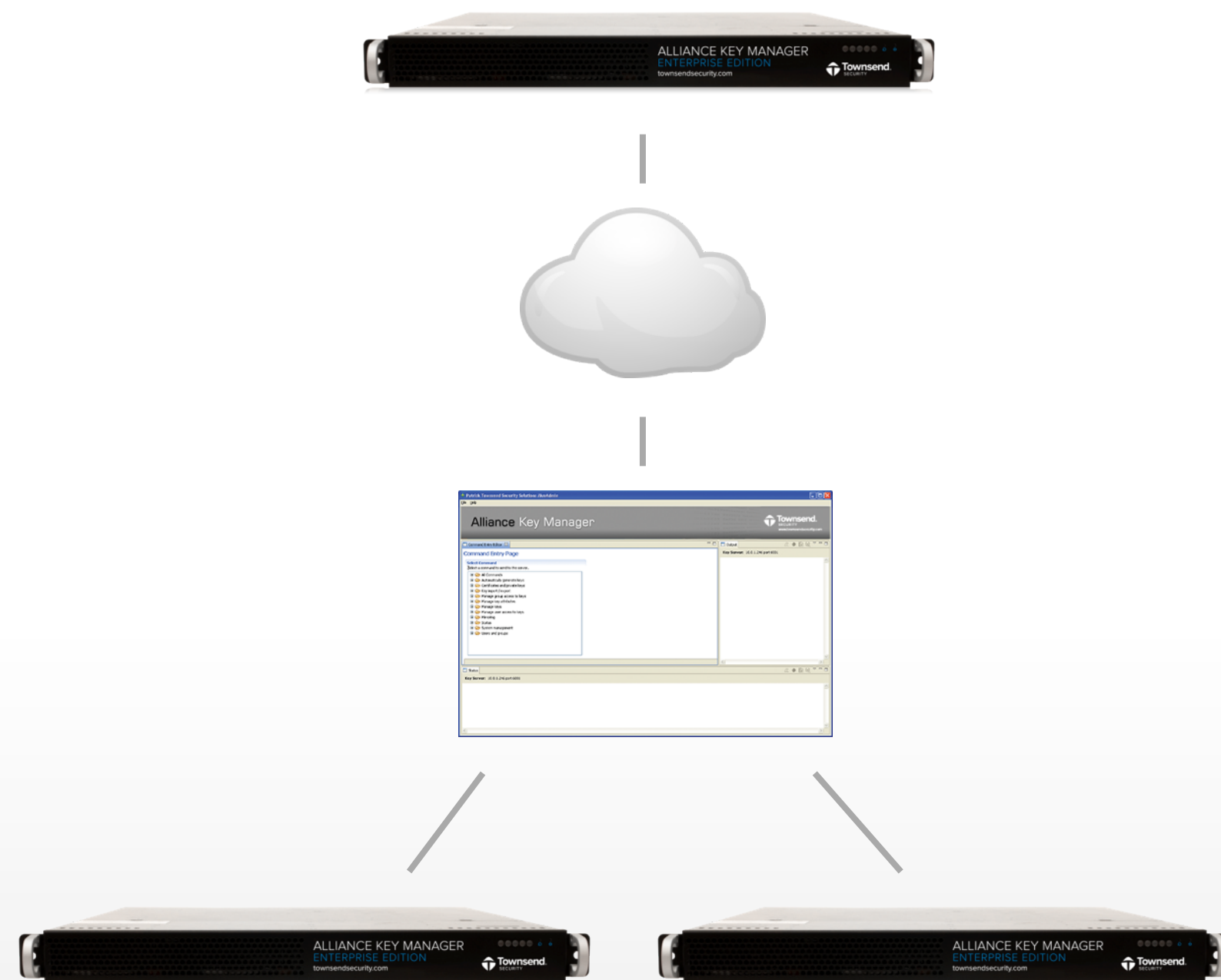
## Key Management *Everywhere* Your Data Is

- Central Key Manager
- Multiple OS support – IBM i, Windows, Linux, Unix, IBM z
- Multiple platforms – Client, server, cloud, mobile, etc.
- Multiple database support – DB2, SQL Server, Oracle, MySQL, etc.
- Multiple application support – FIELDPROC, SQL Server EKM and TDE, Oracle TDE, SharePoint TDE and RBS, etc.



## High Availability

- Key mirroring
- One-way or bi-directional mirroring
- Access policy mirroring
- Configuration mirroring
- Load balancing
- Complex networks
  - Hub-and-spoke
  - Meshed



## Business Continuity

- Backup and recovery
- Backup on schedule
- Secure transfer of DEK and KEK
- Backup and restore audit



## Key Management Built on RESTful APIs

- Easy integration
- Developer-friendly
- Pull keys from anywhere

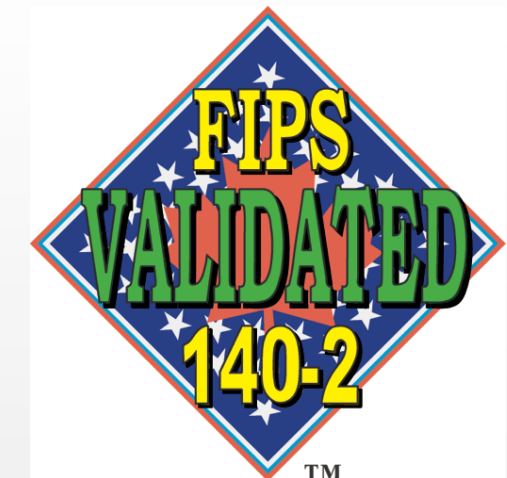
## KMIP

- Key Management Interoperability Protocol (KMIP)
- OASIS standards group
- Base interoperability with extensible functions
- This is a “wire” communication protocol using TLS

The letters "KMIP" in a bold, blue, sans-serif font, enclosed within a thin blue rectangular border.

## NIST FIPS 140-2 Key Management Standard

- Crypto-module standard published by NIST
- NIST tests every aspect of key management: encryption algorithm, key Management RNG, physical security, and much more
- NVLAP independent review and assessment
- Multiple levels (1 through 4)
- Validated solutions: meet non-regulatory, minimum government standards, are re-tested over time, help you meet compliance regulations, have provably secure technology.

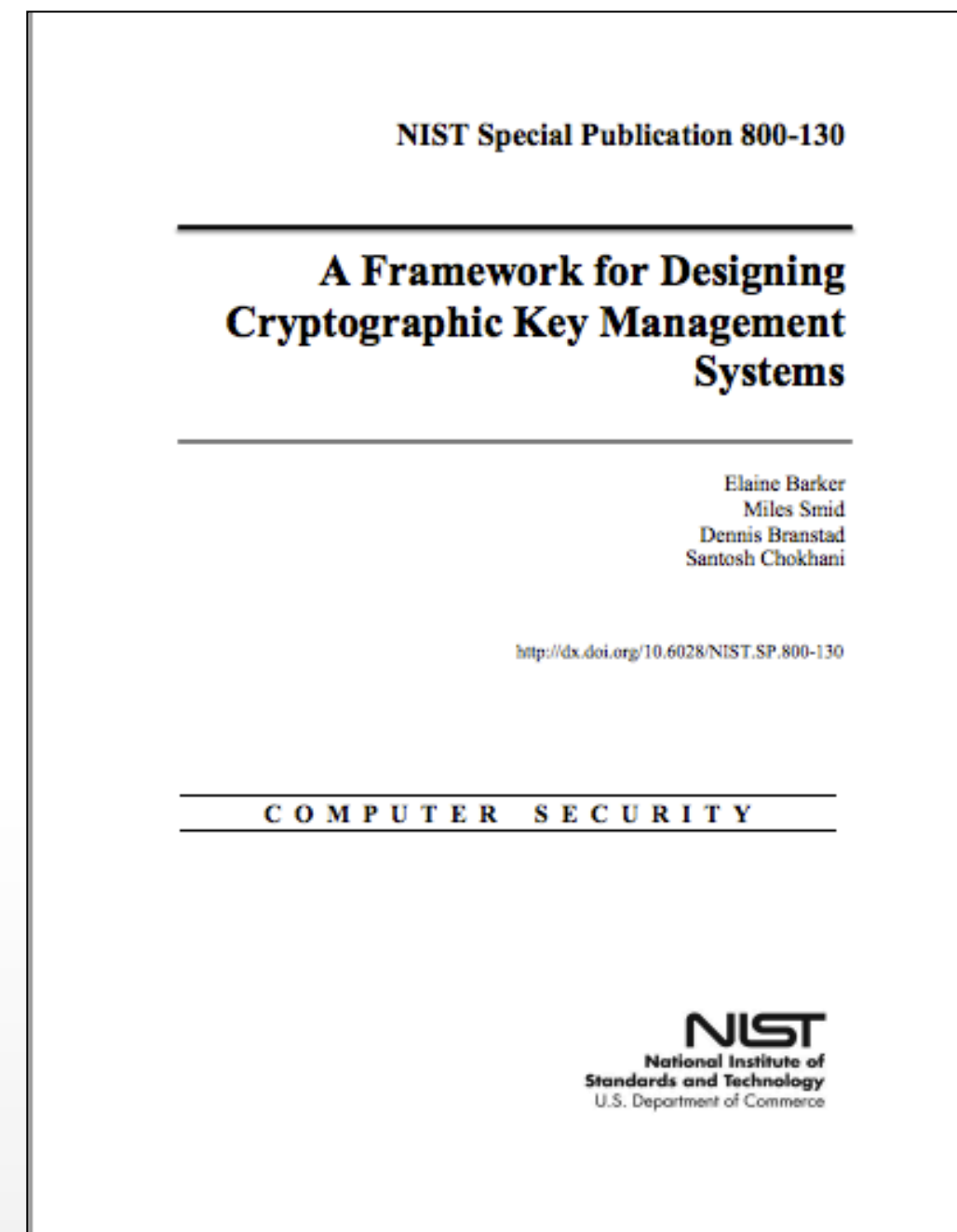


Information is publicly available on the NIST web site:

<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>

## NIST Guidance – A Wakeup Call

- Special Publication 800-130
- Framework for Designing Cryptographic Key Management Systems
- Checklist to evaluate vendor claims



<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf>

## Key Management Best Practices

- Defined by Special Publication SP 800-57 Best Practices for Key Management
- Recommendations for Key Management – Three part document
- Best practices for managing keys, policy and security planning
- Approved cryptographic algorithms and their strengths, factors affecting crypto-periods, key life cycle, audit and recovery, documented policy and procedures, and TLS recommendations.

## Robust Support from Vendor

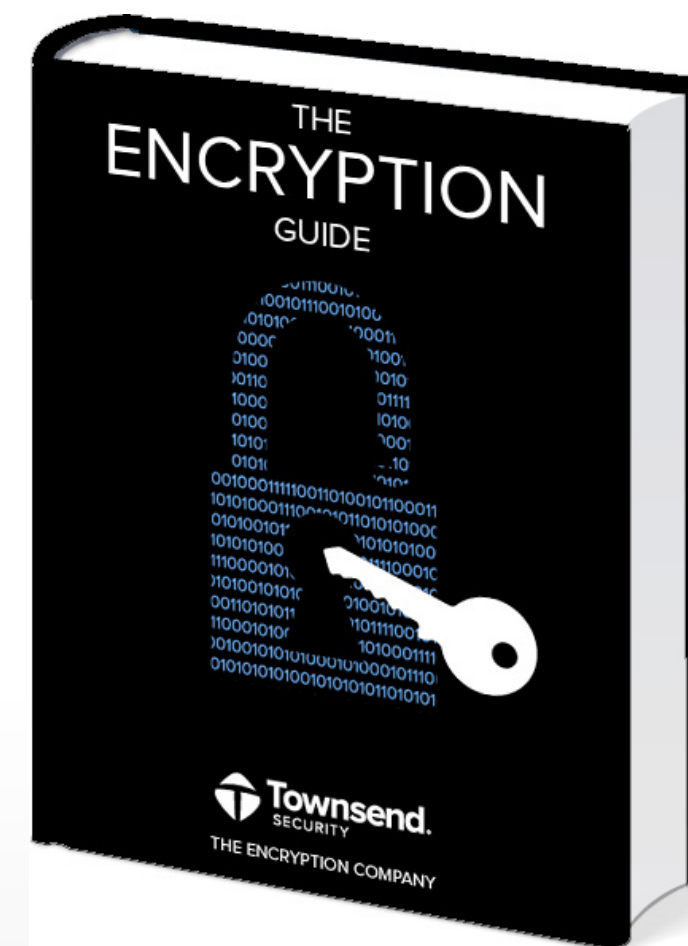
- What are the challenges that storage vendors run into when partnering for key management?
  - Complex agreements with onerous requirements
  - Inability to match business needs with key management vendor distribution practices
  - No support for all target platforms: HSMs, Cloud HSMs, VMware, cloud (AWS, Azure, etc.)
  - Lack of SDKs and sample code
  - Poor customer support – you need 24/7/365



## Any Questions on Encryption Key Management?

### eBook Available

For more information on encryption and key management  
[download this eBook!](#)



### Contact Liz Townsend

[liz.townsend@townsendsecurity.com](mailto:liz.townsend@townsendsecurity.com)