



Education

# Practical Secure Storage: A Vendor Agnostic Overview

Walt Hubis

- ❖ The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- ❖ Member companies and individual members may use this material in presentations and literature under the following conditions:
  - ◆ Any slide or slides used must be reproduced in their entirety without modification
  - ◆ The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- ❖ This presentation is a project of the SNIA Education Committee.
- ❖ Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- ❖ The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

**NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.**

## ➤ Practical Secure Storage: A Vendor Agnostic Overview

- ◆ This presentation will explore the fundamental concepts of implementing secure enterprise storage using current technologies. This tutorial will focus on the implementation of a practical secure storage system, independent of any specific vendor implementation or methodology. The high level requirements that drive the implementation of secure storage for the enterprise, including legal issues, key management, current technologies available to the end user, and fiscal considerations will be explored in detail. In addition, actual implementation examples will be provided that illustrate how these requirements are applied to actual systems implementations.

- Why Encrypt?
- What to Encrypt
- Where to Encrypt
- Key Management

## ➤ Define the Drivers

- ◆ Regulatory Obligations
- ◆ Legal Requirements
- ◆ Corporate Requirements for Confidentiality
- ◆ IS/IT Requirements

- Sarbanes-Oxley
- HIPPA
- Payment Card Industry (PCI-DSS)
- EU Data Privacy
- Industry Specific Requirements
- Country Specific Requirements

- Court Orders
- Contractual Obligations
- Due Care
- Trade Secrets
- Competitively Sensitive Information
- National Security
- Intellectual Property

## ➤ Management Concerns

- ◆ Public Image
- ◆ Thwarting/Detecting Criminal Activity
- ◆ Protecting Intellectual Property
- ◆ Traceability to Quantifiable Obligations and Requirements

## ➤ Organizational Policies

- ◆ Retention
- ◆ Destruction
- ◆ Privacy/Confidentiality



## ➤ IS/IT

- ◆ Compliance with Strategic Plan
- ◆ Desired Future States
- ◆ Audit Results

## ➤ Monitoring

- ◆ Track Access to Sensitive Data
- ◆ Monitor Intrusion

## ➤ Audits

- ◆ May be an Additional Legal or Corporate Obligation

## ➤ Valuable Data

- ◆ Redundancy
- ◆ Disaster Protection
- ◆ Replication

## ➤ Sensitive Data

- ◆ Confidentiality
- ◆ Access Control
- ◆ Integrity
- ◆ Immutability

- Organizational Confidentiality Priorities
- Confidentiality Categories
  - ◆ Most Confidential
  - ◆ Competitively Sensitive
  - ◆ Personally Identifiable information (PII)
  - ◆ Top Secret
  - ◆ Restricted Financial
  - ◆ Etc.

# Data Assets Inventory

## ➤ Applications

- ◆ Generate, process, modify, and preserve the data

## ➤ Hosts/Servers

- ◆ Include operating systems
- ◆ Access, use, and store the data
- ◆ Storage Devices

## ➤ Data Owners

- ◆ Custodians, stakeholders, and business units
- ◆ Vested interest in the protection measures and a need to access the data

- Networks
- Geographic Locations
- Risk Assessment
  - ◆ Where's your security boundary?

- Temporary Storage
- Caches
- Data Mirrors (Replication)
- Mobile Devices
- Backup/Archives
- Compression/DeDuplication

# Points of Encryption

## ➤ Application Level

- ◆ Application
- ◆ Database

## ➤ File System Level

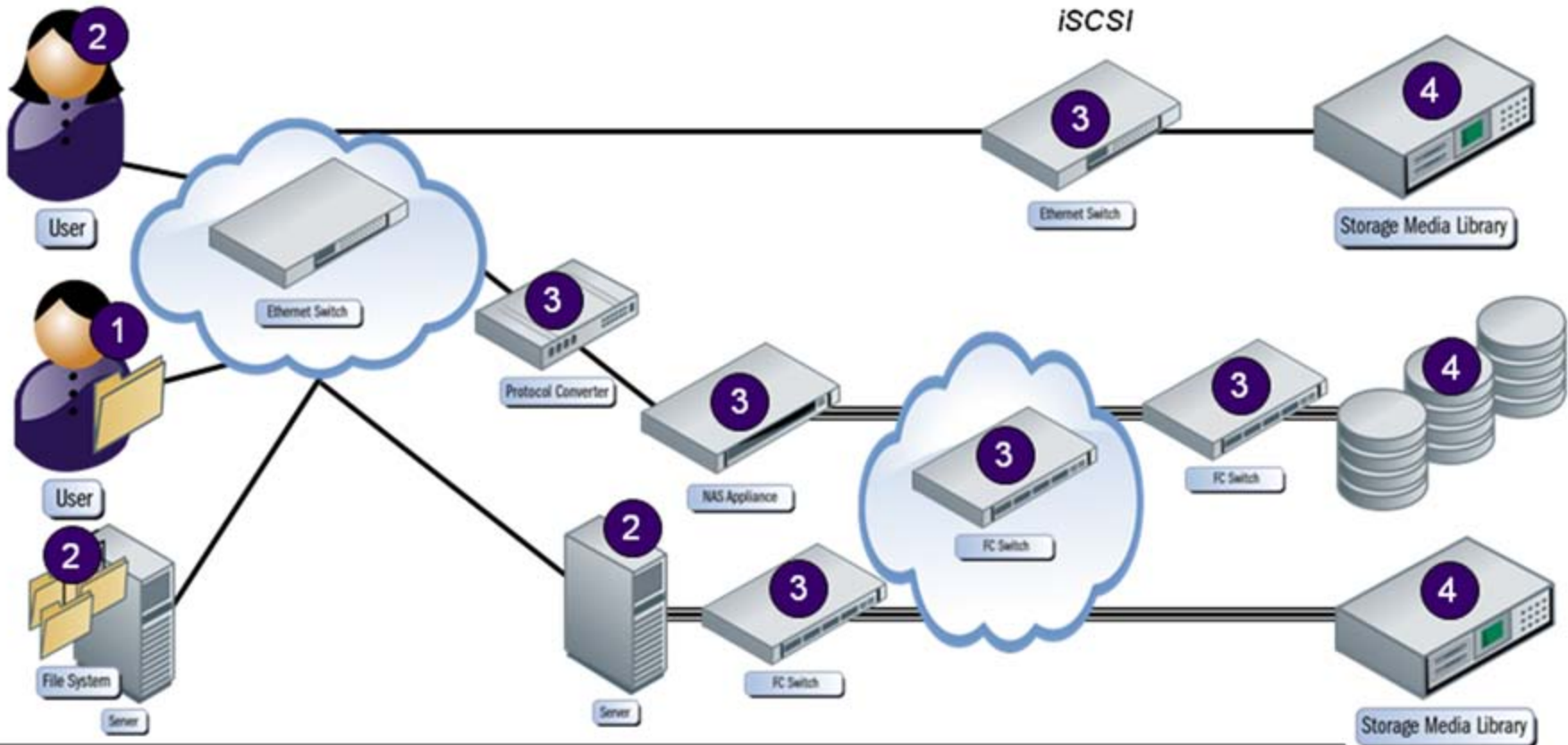
- ◆ OS
- ◆ OS-level application

## ➤ HBA, Array Controller, or Switch Level

- ◆ File-based (NAS)
- ◆ Block Based

## ➤ Device Level

# Where to Encrypt

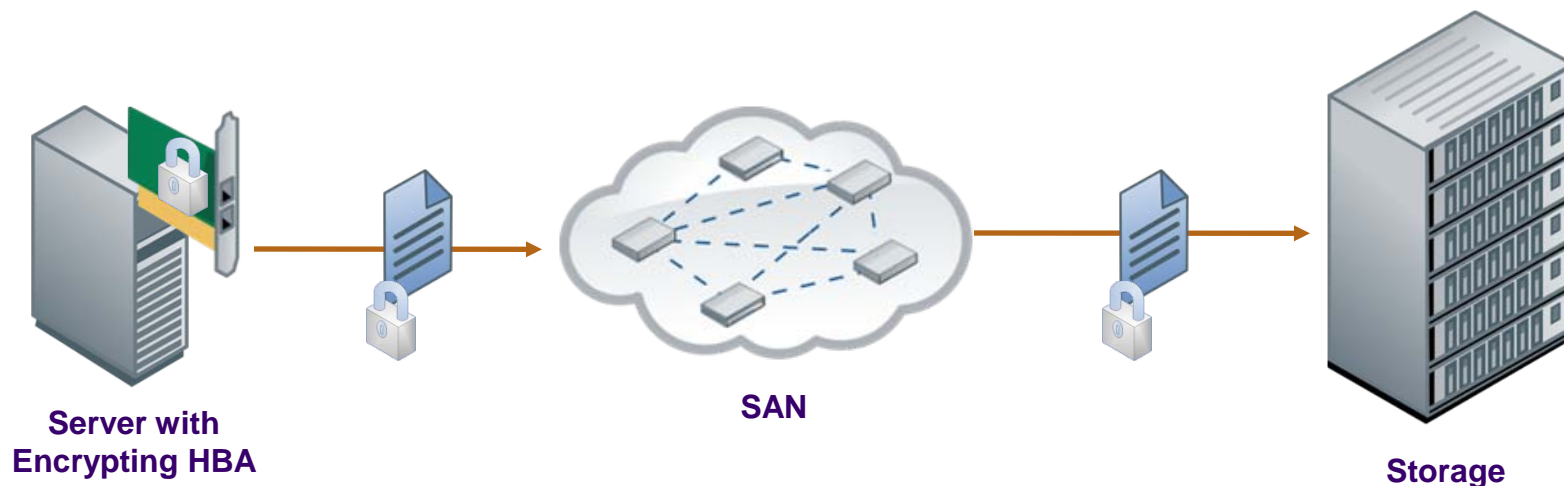


- |                            |  |
|----------------------------|--|
| <b>1</b> Application-level | <b>3</b> HBA-, Array Controller- or Switch-level |
| <b>2</b> Filesystem-level  | <b>4</b> Device-level                            |

Source: SNIA Security Work Group, *Encryption of Data At-Rest*, Version 2.0, September 9, 2009

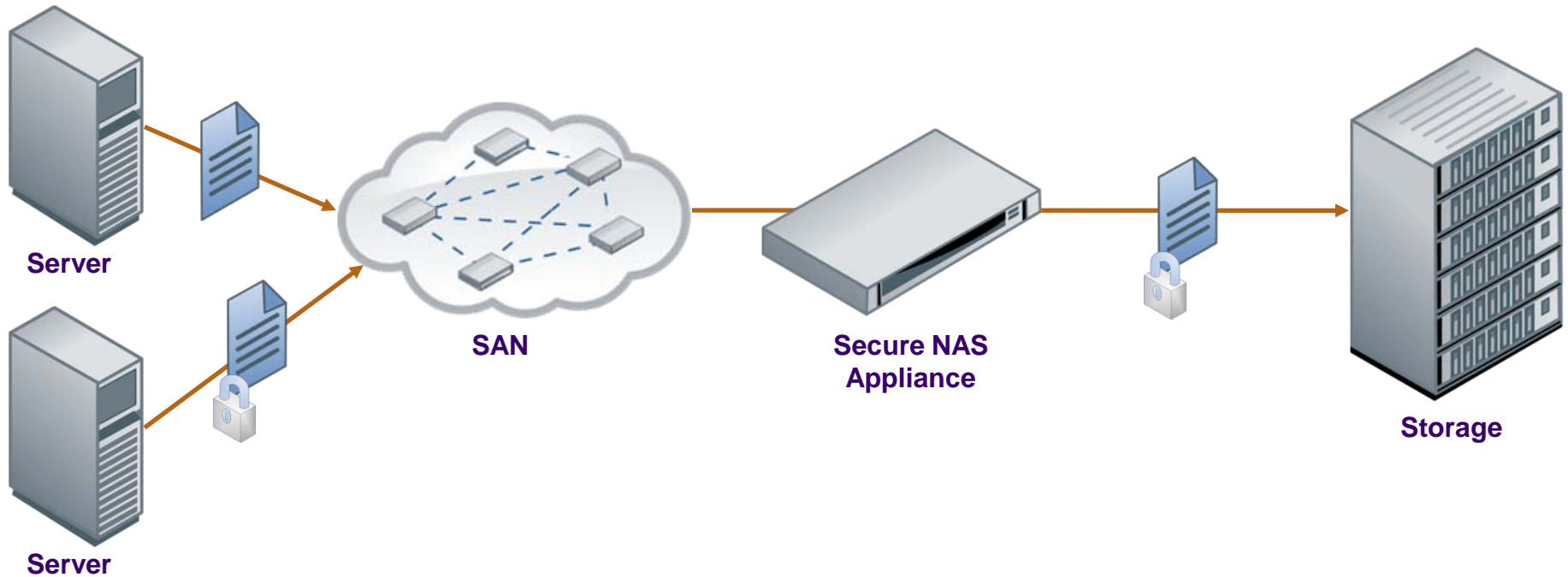


# HBA Encryption



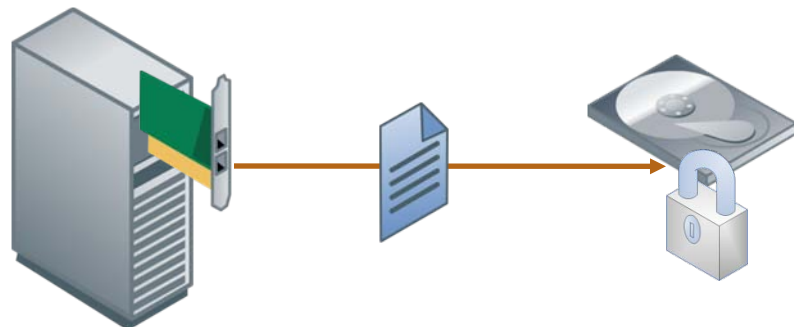
- Data Encrypted End to End
- Problems with De-Duplication and Compression
- Data is Encrypted In-Flight
- Key management issues
  - ◆ Ephemeral Keys for In-Flight Data
  - ◆ Long-Lived Keys for Data at Rest Encryption

# Secure Appliance



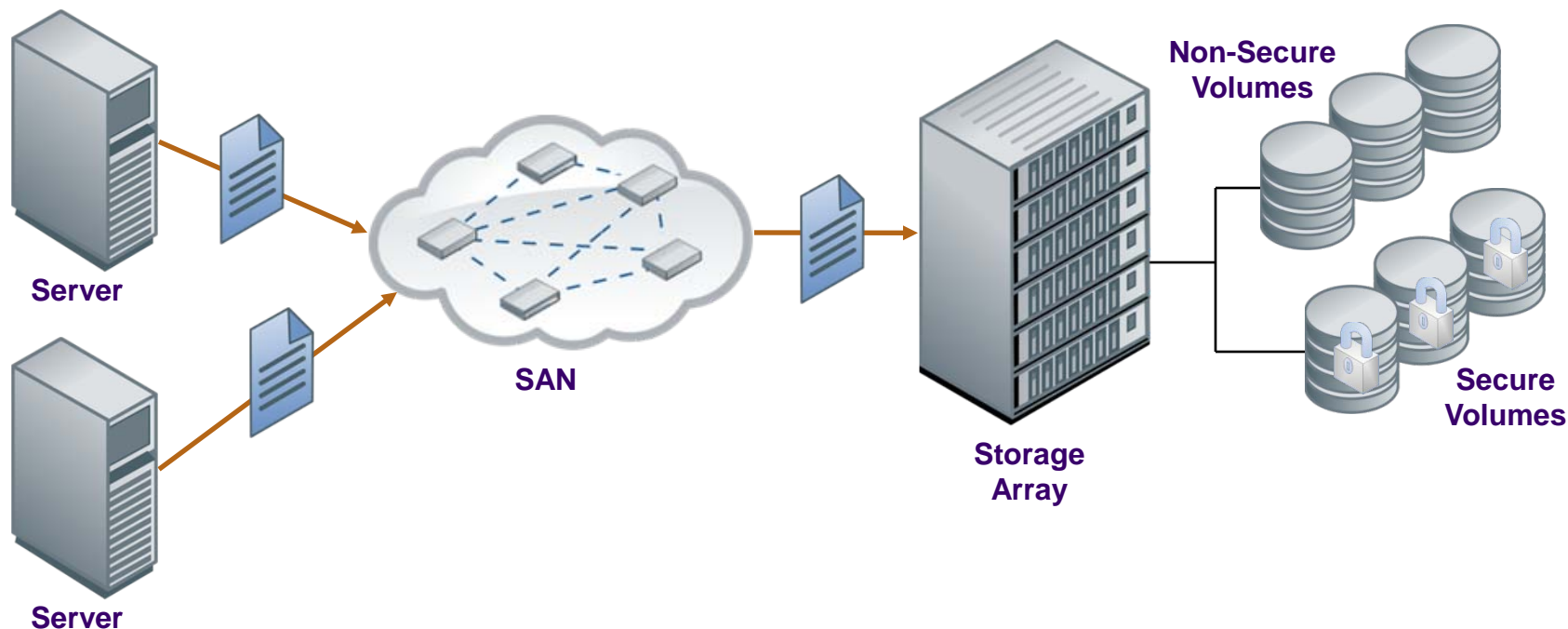
- Data May Be Encrypted End to End
- Highly Secure Solutions Possible
- Scalability may be an Issue

# Secure Disk (DAS)



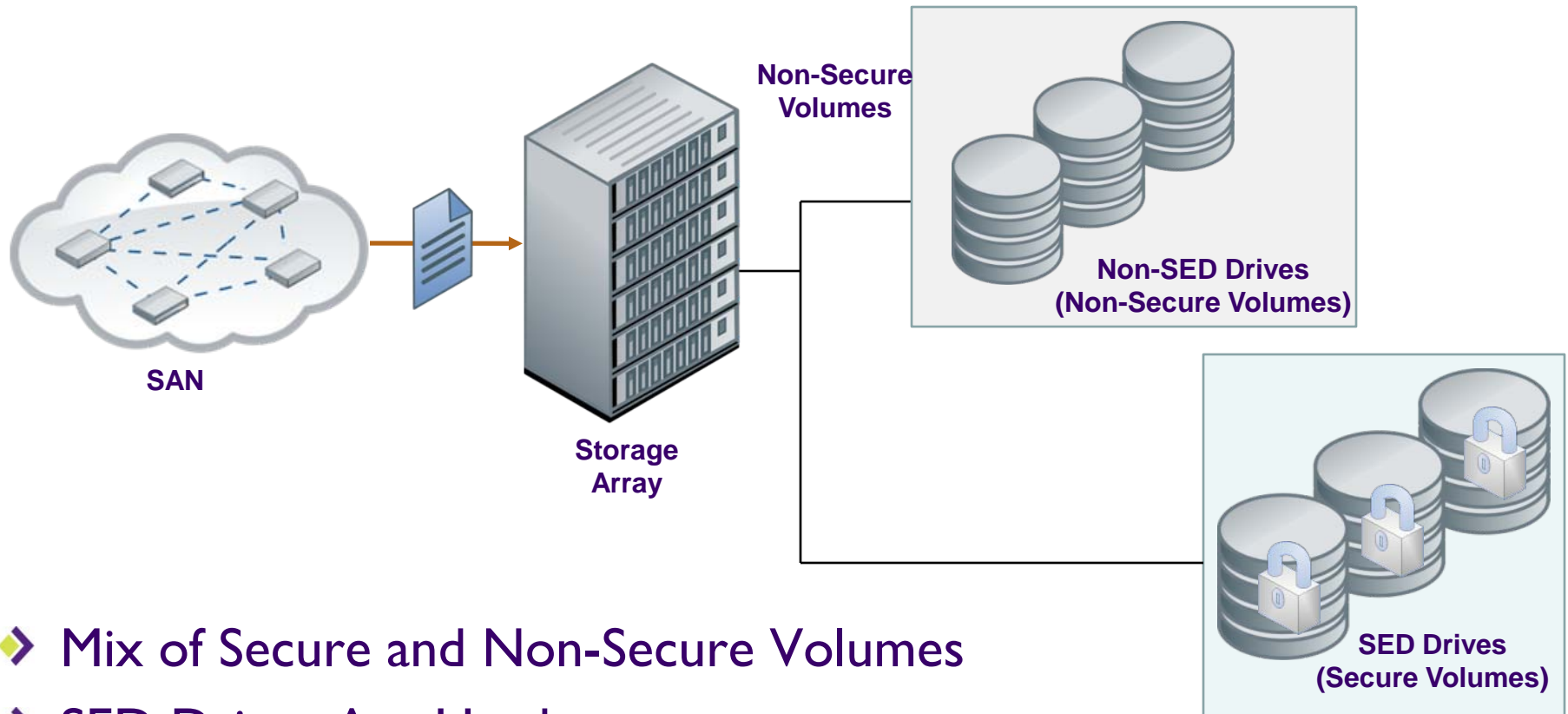
- Self-Encrypting Disk
- Direct Attach Storage (DAS)
- Issues with SED DAS as boot device
- Provide theft or loss protection
- Inexpensive

# Secure Disk (NAS)



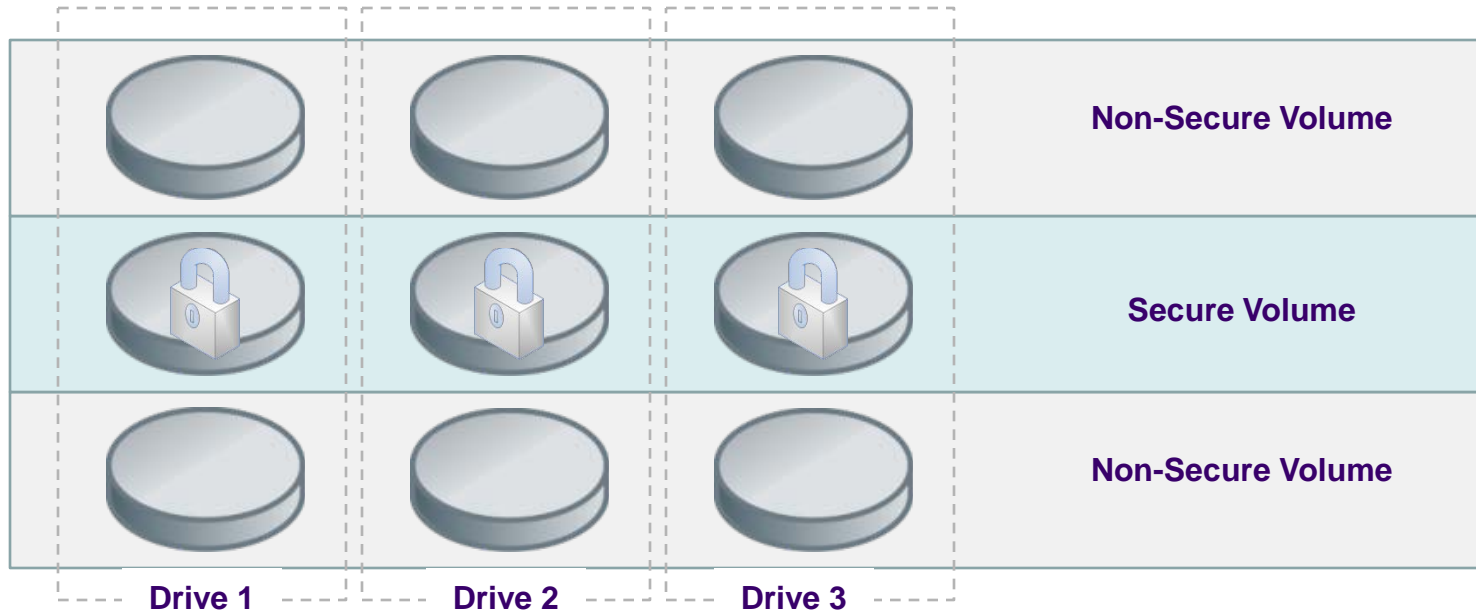
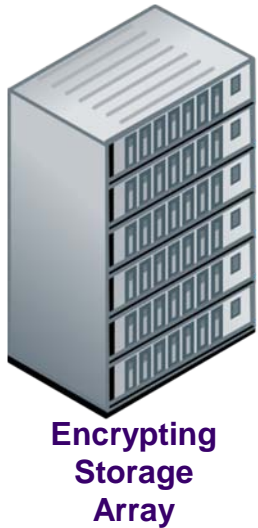
- Encryption at Storage Array
- Protection for Loss or Theft of Disks

# Array with SED Drives

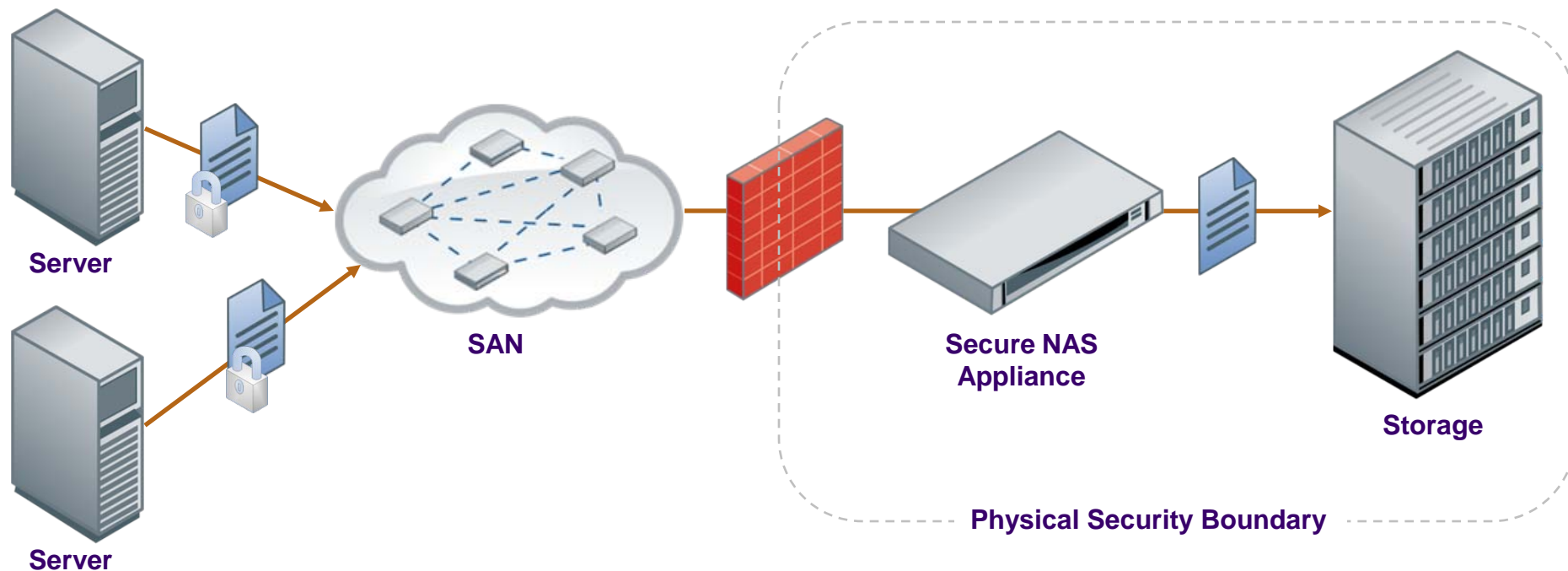


- Mix of Secure and Non-Secure Volumes
- SED Drives Are Used
- All Volumes on Drives are Secure

# Encrypting Array



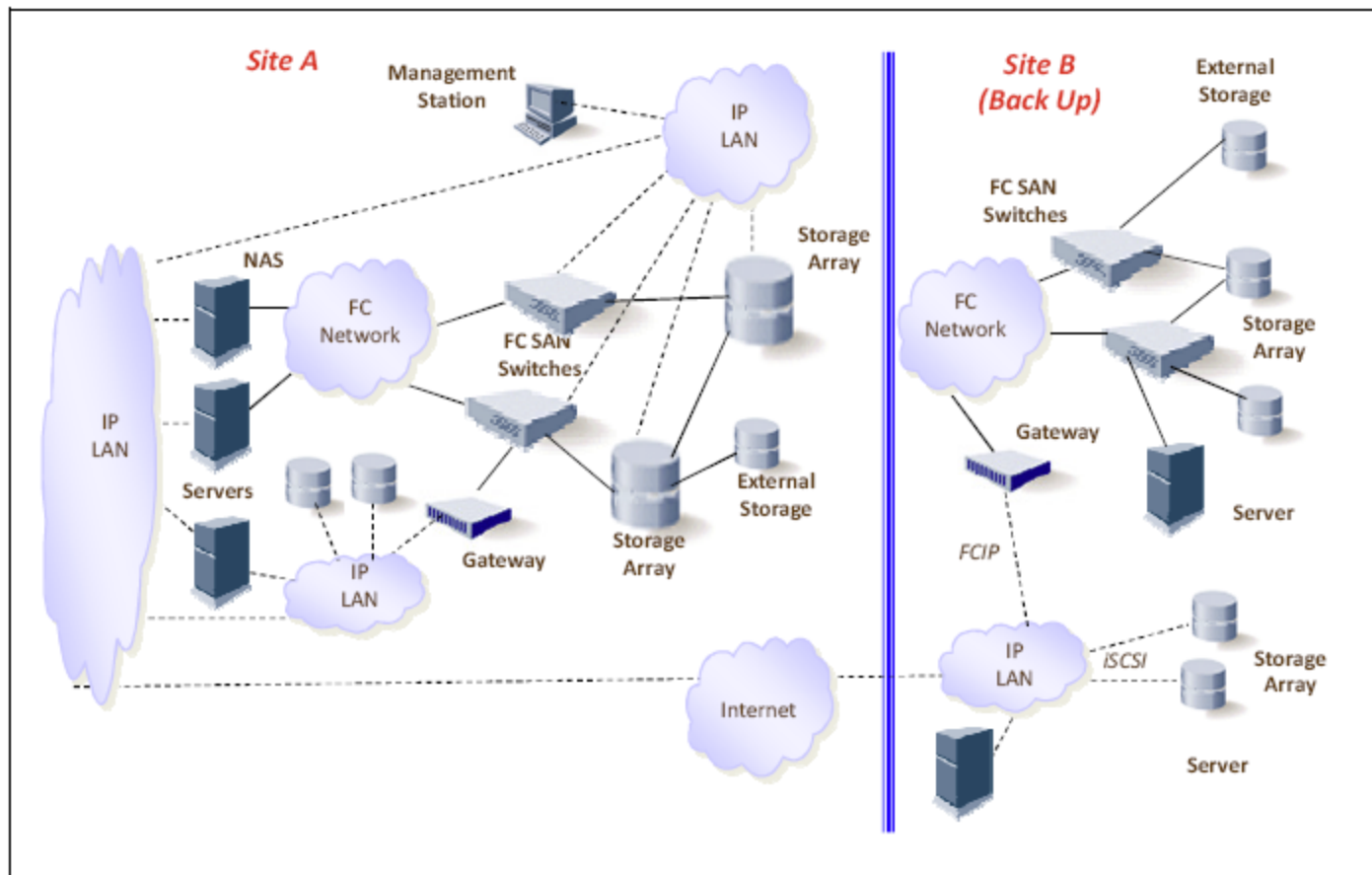
- Mix of Secure and Non-Secure Volumes
- Non-Encrypting Drives Are Used
- Secure and Non-Secure Volumes on a single drive



## ➤ Data must be secured across boundary

- ◆ Electronic Data
- ◆ Physical Data (tapes, drives, etc.)

# Geographic Security Boundaries

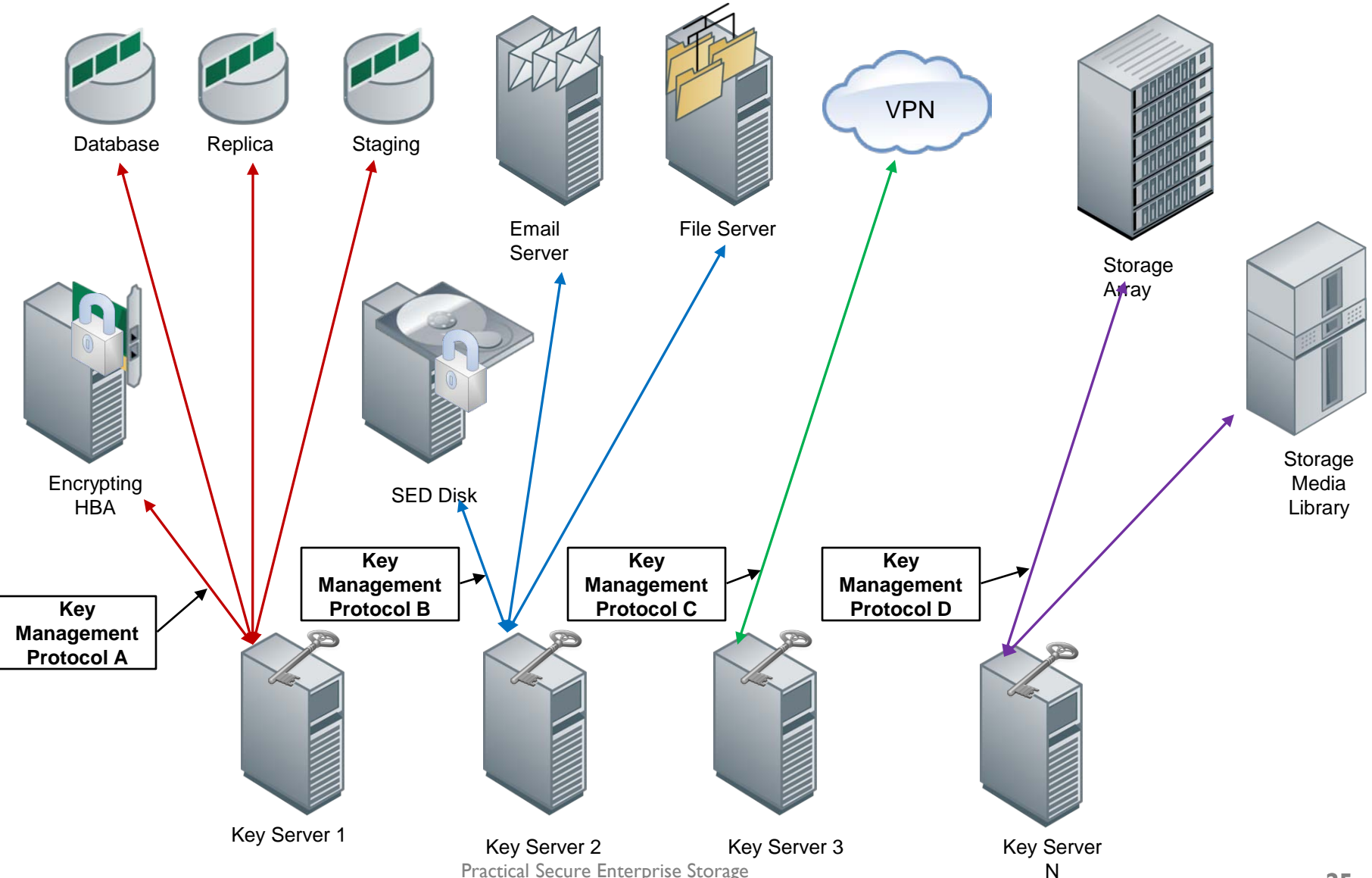


## ➤ Data Movement across borders can be problematic

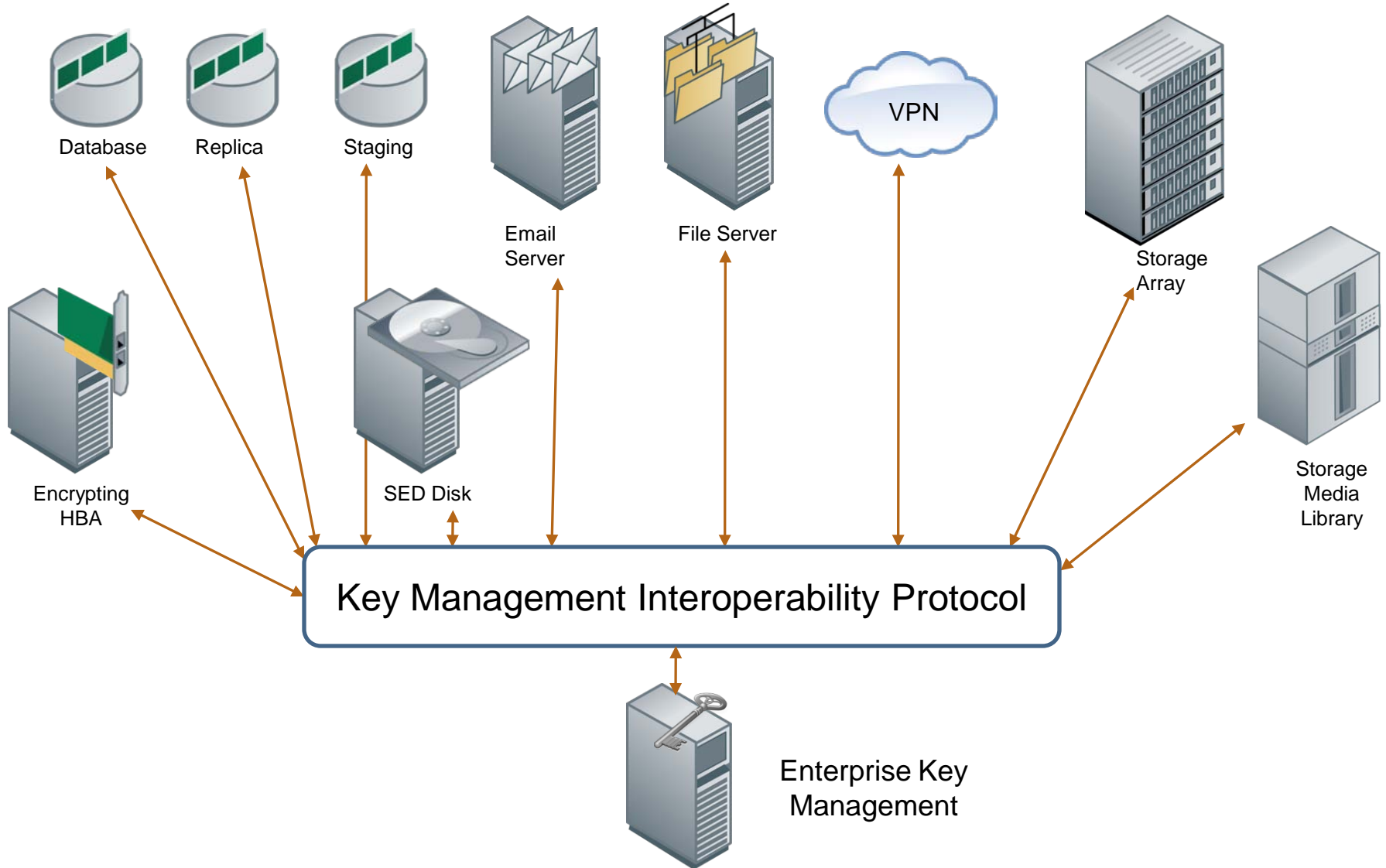
Source: SNIA Security Work Group, *Legal Issues for Storage*, Version 1.0, September 29, 2009



# Key Management



# Standardized Key Management



## ➤ Many Key Uses

- Private signature key
- Public signature verification key
- Symmetric authentication key
- Private authentication key
- Public authentication key
- Symmetric data encryption key
- Symmetric key wrapping key
- Symmetric and asymmetric random number generation keys
- Symmetric master key
- Private key transport key
- Public Key Transport Key
- Symmetric Key Agreement Key
- Private Static Key Agreement Key
- Public Static Key Agreement Key
- Private Ephemeral Key Agreement Key
- Public Ephemeral Key Agreement Key
- Symmetric Authorization Key
- Private Authorization Key
- Public Authorization Key

Source: NIST Special Publication 800-57: Recommendation for Key Management Part 1: General

## ➤ Encryption Algorithms

- ◆ AES
  - › 128 Bit Key
  - › 192 Bit Key
  - › 256 Bit Key
- ◆ DES
  - › 56 Bit Key
- ◆ 3DES
  - › 168 Bit Key

## ➤ Encryption Algorithm Modes

- ◆ Electronic Codebook Mode (ECB)
- ◆ Cipher Block Chaining Mode (CBC)
- ◆ Cipher Feedback Mode (CFB)
- ◆ Output Feedback Mode (OFB)
- ◆ Counter Mode (CTR)
- ◆ Galois/Counter Mode (GCM)
- ◆ LRW Encryption
- ◆ XOR-Encrypt-XOR (XEX)
- ◆ XEX-TCB-CTS (XTS)
- ◆ CBC-Mask-CBC (CMC)
- ◆ ECB-Mask-ECB (EME)

# Key Management Issues

- Key Management Issues
  - ◆ Confidentiality
  - ◆ Integrity
  - ◆ Availability
  - ◆ Misuse
- Disclosure of Key is Disclosure of Data
- Loss of Key is Loss of Data
- Key Availability is Data Availability

# Key Management Guidelines

- Use a Cryptographic Key for One Purpose
  - ◆ Ephemeral Keys for Data in Flight
  - ◆ Long-Lived Keys for Data at Rest
  - ◆ Keep Data Encryption and Other Keys Separate
- Use Randomly Chosen Keys
- Use Entire Key Space
- Avoid Weak Keys
- Avoid Plain Text Keys

# Questions

# For More Information

- **SNIA: Introduction to Storage Security**  
([http://www.snia.org/forums/ssif/knowledge\\_center/white\\_papers/Storage-Security-Intro-2.0.090909.pdf](http://www.snia.org/forums/ssif/knowledge_center/white_papers/Storage-Security-Intro-2.0.090909.pdf))
- **SNIA: Audit Logging for Storage**  
([http://www.snia.org/forums/ssif/knowledge\\_center/white\\_papers/forums/sif/knowledge\\_center/white\\_papers/SNIA-Logging-VWP.050921.pdf](http://www.snia.org/forums/ssif/knowledge_center/white_papers/forums/sif/knowledge_center/white_papers/SNIA-Logging-VWP.050921.pdf))
- **Encryption of Data at Rest: A Step by Step Checklist**  
([http://www.snia.org/forums/ssif/knowledge\\_center/white\\_papers/Encryption-Checklist-2.0.090909.pdf](http://www.snia.org/forums/ssif/knowledge_center/white_papers/Encryption-Checklist-2.0.090909.pdf))
- **SNIA: Best Practices for Deploying a Storage Security Solution**  
([http://www.snia-europe.org/news\\_events/e\\_news/](http://www.snia-europe.org/news_events/e_news/))



# For More Information

- NIST Special Publication 800-57: Recommendation for Key Management ([http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2\\_Mar08-2007.pdf](http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf))
- ISO/IEC 11770 Parts 1-3: Information technology - Security techniques - Key management (<http://webstore.ansi.org/> )
- FIPS 140-2: SECURITY REQUIREMENTS MODULES (<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>)
- Trusted Computing Group (<https://www.trustedcomputinggroup.org/home>)
- IEEE P1619.3: Security in Storage Workgroup (SISWG) Key Management Subcommittee (<http://siswg.net/>)
- OASIS Enterprise Key Management Infrastructure (EKMI) Technical Committee ([http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=ekmi](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ekmi))
- IETF: Provisioning of Symmetric Keys (KEYPROV) (<http://www.ietf.org/html.charters/keyprov-charter.html>)

## ➤ SNIA Security Technical Work Group (TWG)

- ◆ Focus: Requirements, architectures, interfaces, practices, technology, educational materials, and terminology for storage networking.
- ◆ [http://www.snia.org/tech\\_activities/workgroups/security/](http://www.snia.org/tech_activities/workgroups/security/)

## ➤ Storage Security Industry Forum (SSIF)

- ◆ Focus: Educational materials, customer needs, whitepapers, and best practices for storage security.
- ◆ <http://www.snia.org/ssif>



## **Check out SNIA Tutorials:**

**Introduction to Key Management for Secure Storage**

**An Inside Look at Imminent Key Management Standards**

**Introduction to Storage Security**

**Legal Issues Relevant to Storage**

- Please send any questions or comments on this presentation to SNIA: add your track reflector here

**Many thanks to the following individuals  
for their contributions to this tutorial.**

**- SNIA Education Committee**

**Larry Hofer CISSP  
Eric Hibbard CISSP  
Richard Austin  
Gianna DaGiau**

**SNIA SSIF  
SNIA Security TWG  
Roger Cummings**