Practical Secure Storage: A Vendor Agnostic Overview

Walt Hubis
Hubis Technical Associates

SNIA Legal Notice

- 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.

Abstract

Practical Secure Storage: A Vendor Agnostic Overview

This tutorial will explore the fundamental concepts of implementing secure enterprise storage using current technologies. It has been significantly updated to include current and emerging technologies and changes in international security standards (e.g., ISO/IEC).

The focus of this tutorial is 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.

Overview

- Why encrypt
- What to encrypt
- Where to encrypt
- Key management

Why Encrypt?

- Define the drivers
  - Regulatory obligations
  - Legal requirements
  - Corporate requirements for confidentiality
  - IS/IT requirements
  - Sanitization (cryptographic erasure)
  - Safe harbor (breach notification)

Regulatory Obligations

- US requirements
  - Sarbanes-Oxley
  - HIPAA
  - National security
  - Breach notification (safe harbor)
- Regional requirements
  - EU data privacy
  - EU data protection
- International requirements
  - Basel III Securitisation Framework
  - AML/KYC/CTF
- Industry specific requirements
- Country specific requirements

Legal Obligations

- Court orders
- Contractual obligations
- Payment Card Industry (PCI-DSS)
- Due care
- Trade secrets
- Competitively sensitive information
- Intellectual property

Corporate Requirements

- Management concerns
  - Public image
  - Thwarting/detecting criminal activity
  - Protecting intellectual property
  - Traceability to quantifiable obligations and requirements
- Organizational policies
  - Retention
  - Destruction
  - Privacy/confidentiality
- Governance
  - Privacy
  - E-Discovery
  - Metadata management

Other Requirements

- 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
  - Monitoring
  - Evidence collection

What to Protect

- Valuable data
  - Redundancy
  - Disaster protection
  - Replication
- Sensitive data
  - Confidentiality
  - Access control
  - Integrity
  - Immutability

What and How to Protect

- Organizational confidentiality priorities
- Confidentiality categories
  - Most confidential
  - Competitively sensitive
  - Personally identifiable information (PII)
  - Top secret
  - Restricted financials
  - 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

Data Assets Inventory

- Networks
- Geographic locations
- Risk assessment
  - Where's your security domain?

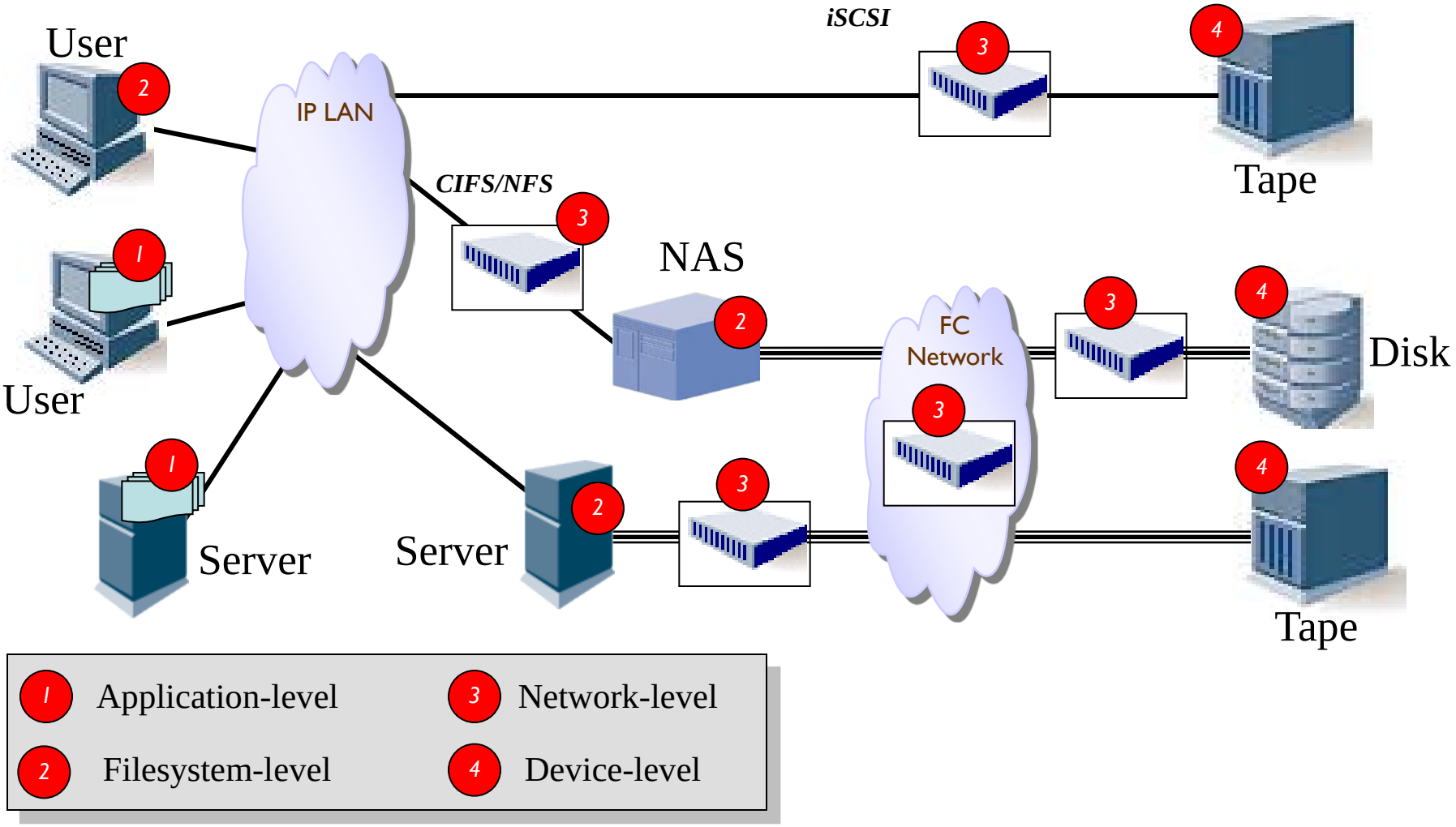
Data Flow

- Temporary storage
- Caches
- Data mirrors (replication)
- Mobile devices
- Backup/archives
- Compression/deduplication

Points of Encryption

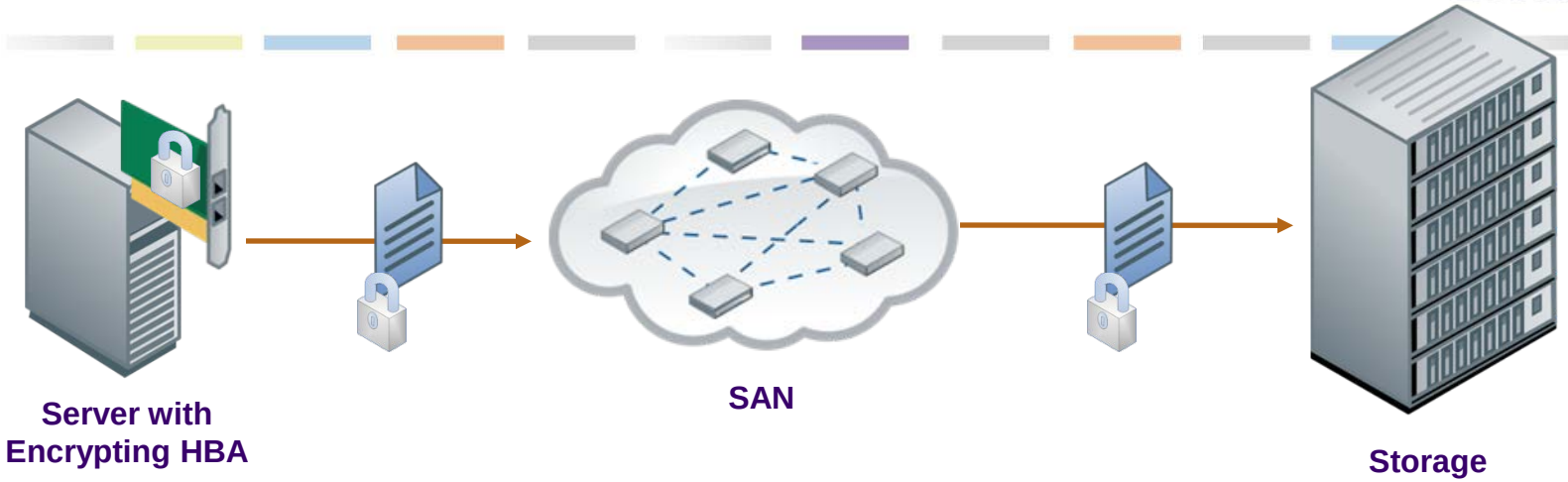
- Application level
  - Application
  - Database
- File system level
  - OS
  - OS-level application
- HBA, array controller, or switch level
  - File-based (NAS)
  - Block based
- Device level
  - Sanitization via cryptographic erase

Where to Encrypt



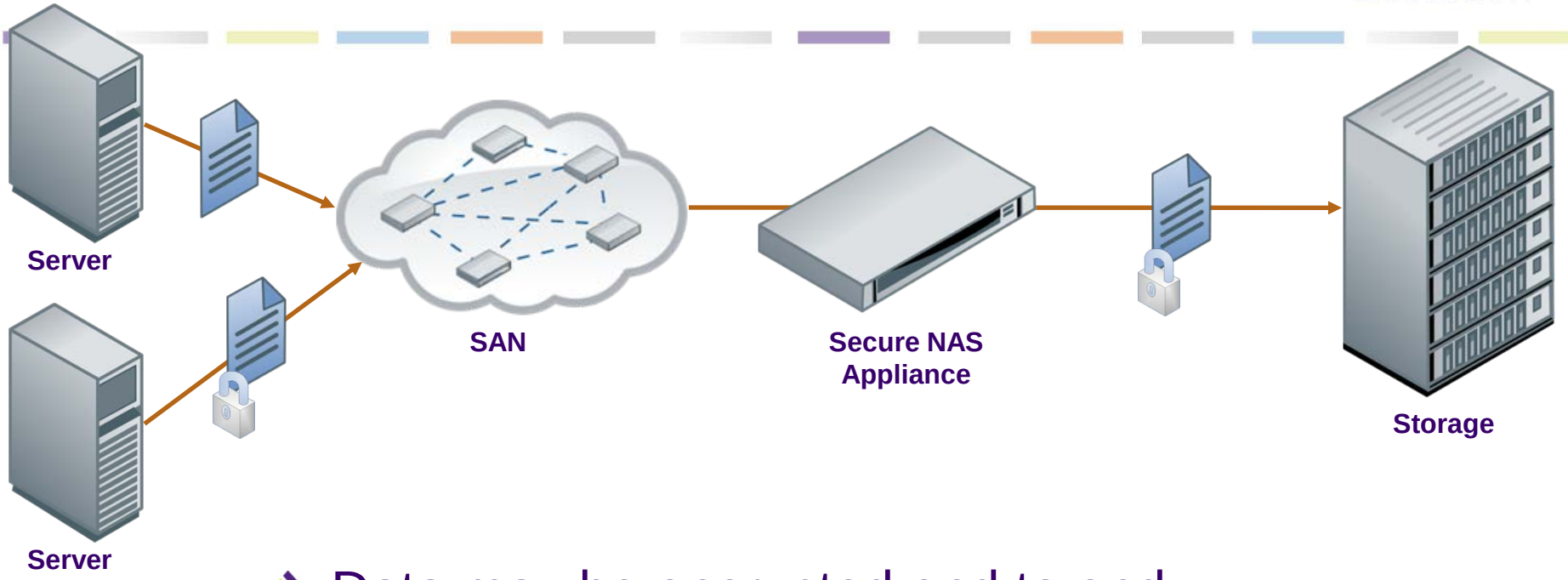
Source: ISO/IEC 27040 - Information technology - Security techniques - Storage security

HBA Encryption



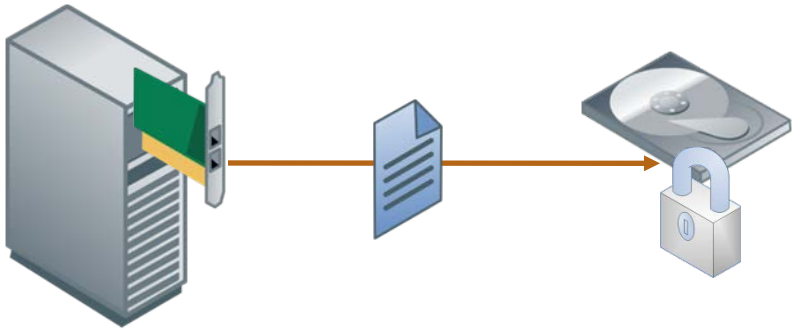
- Data encrypted end to end
- Problems with de-duplication and compression
- Data is encrypted in-flight
- Key management issues
  - Ephemeral keys for in-flight data
  - Long-lived keys for data at rest encryption

Secure Appliance



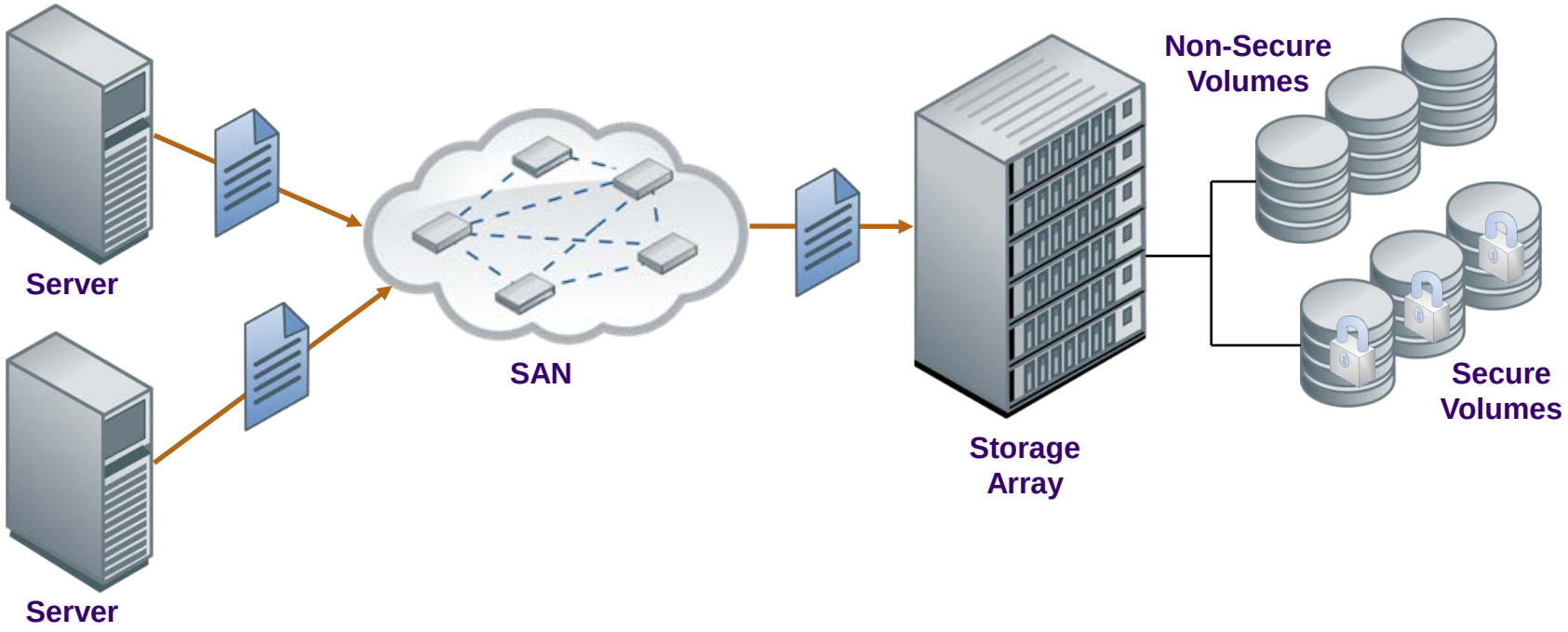
- Data may be encrypted end to end
- Highly secure solutions possible
- Scalability may be an issue

Secure Disk (DAS)



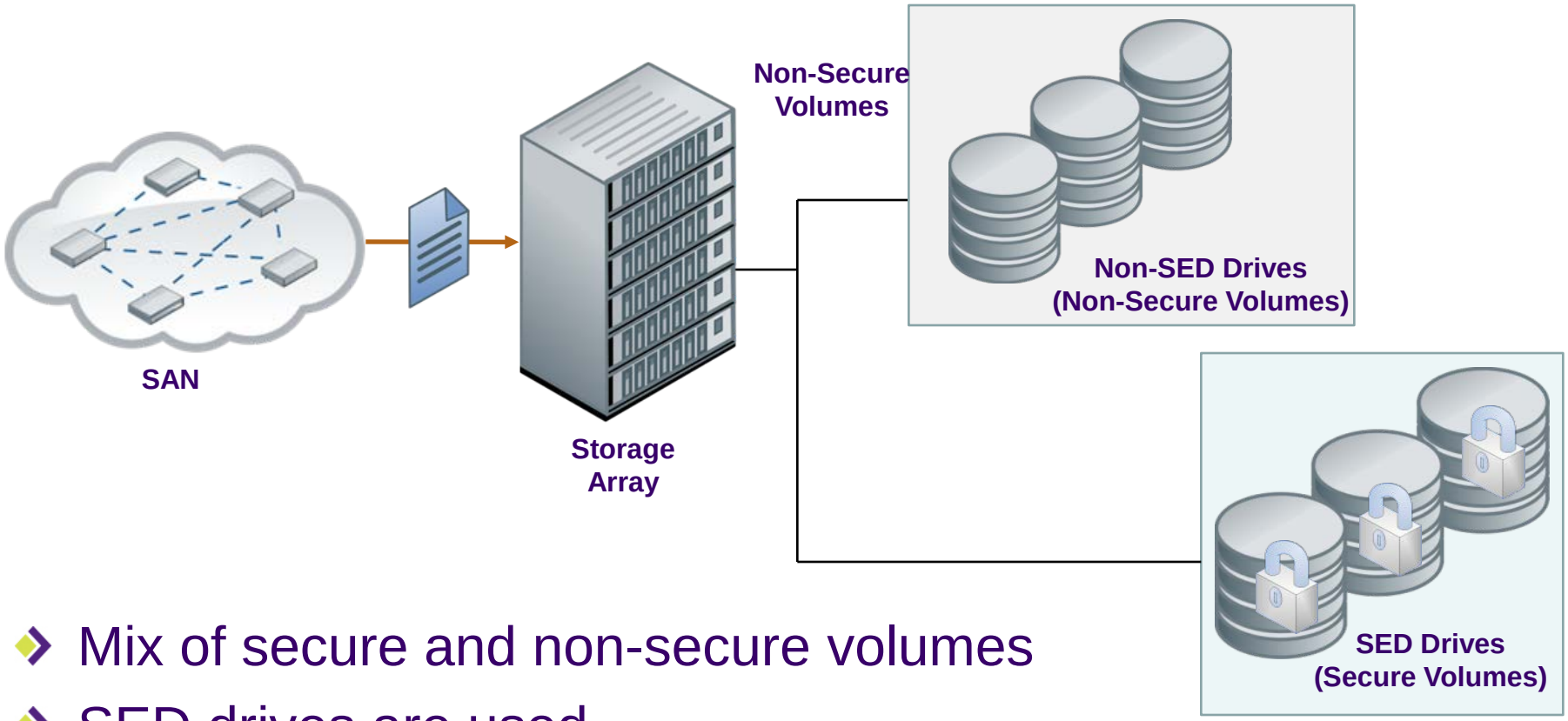
- Self-encrypting disk
- Direct attach storage (DAS)
- Issues with SED DAS as boot device
- Provide theft or loss protection
- Inexpensive

Secure Disk (NAS)



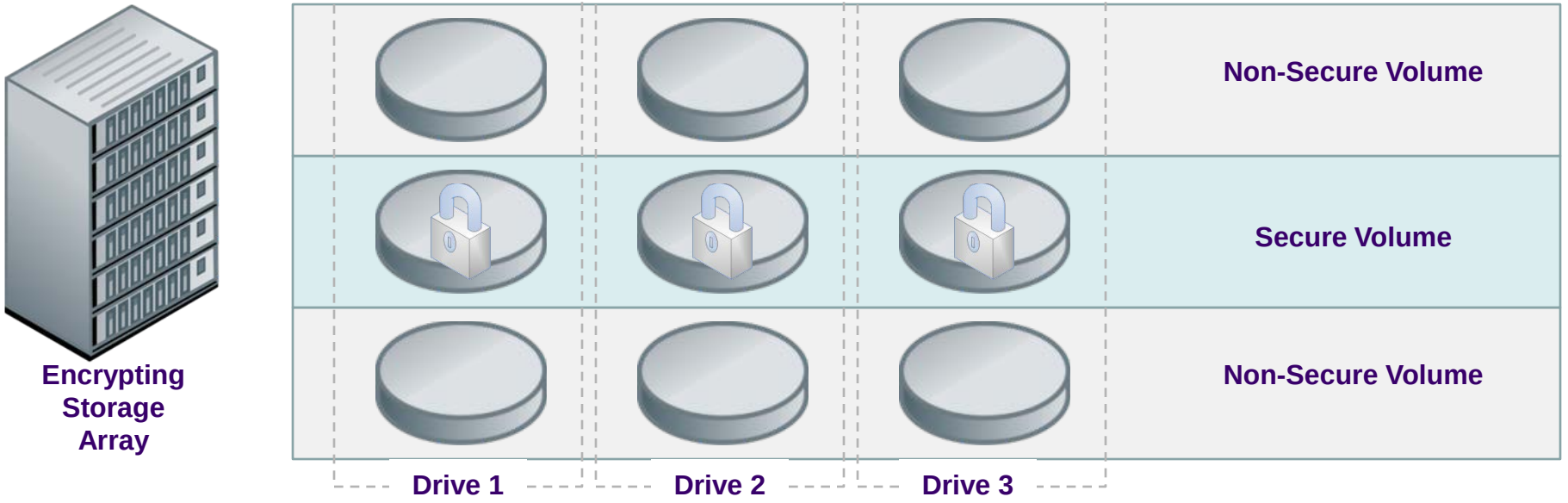
- Encryption at storage array
- Protection for loss or theft of disks

Array with SED Drives



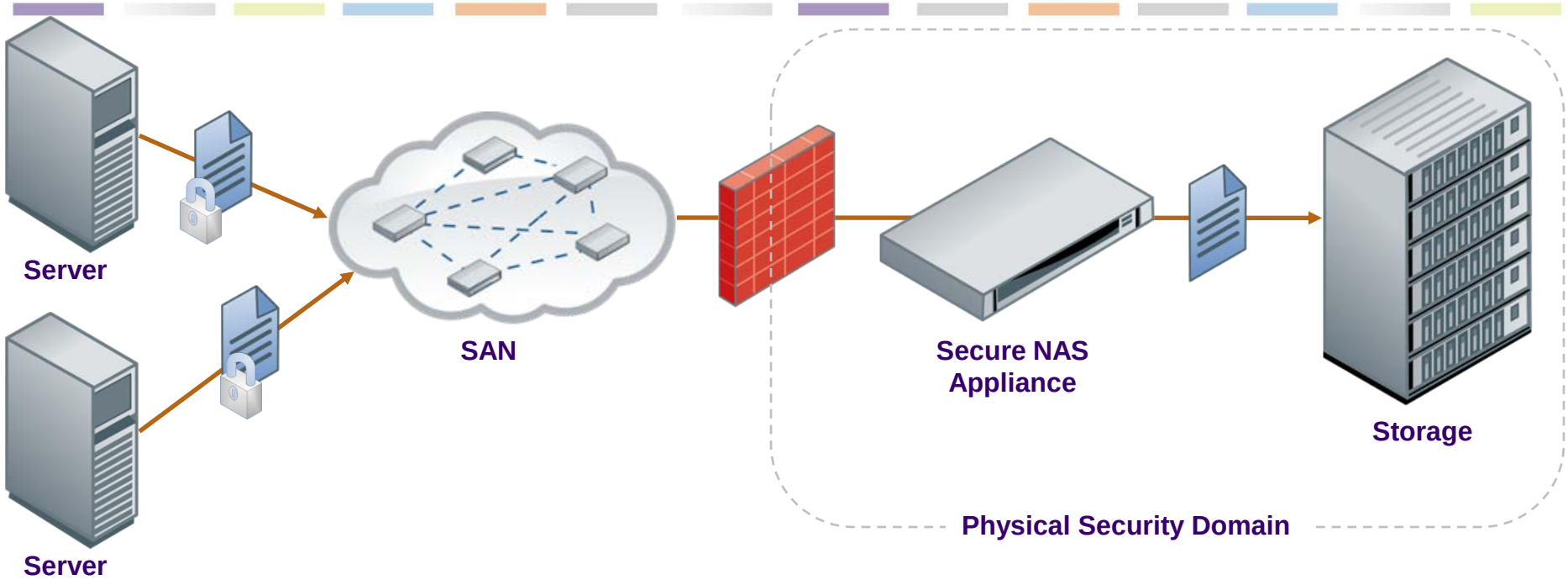
- Mix of secure and non-secure volumes
- SED drives are used
- All volumes on drives are secure

Encrypting Array



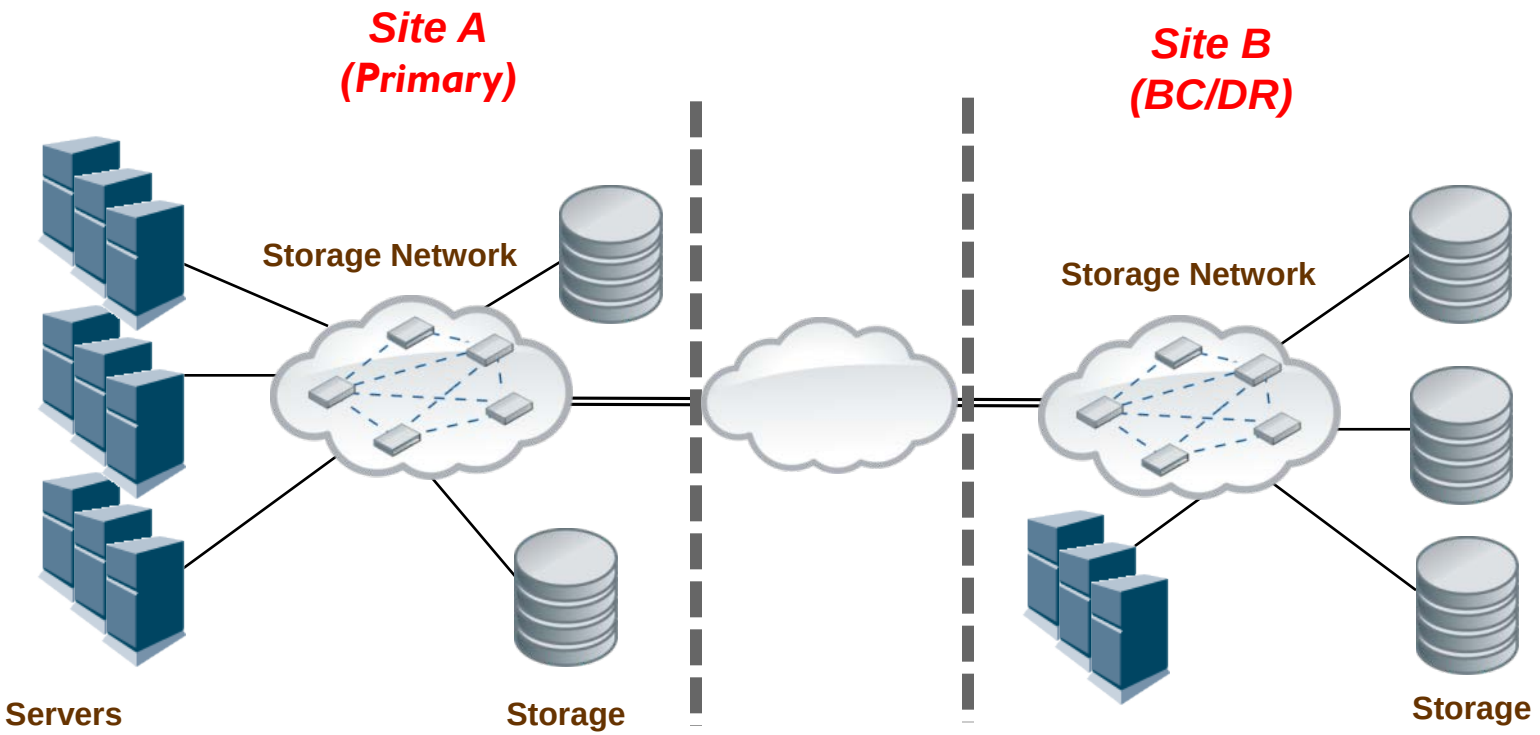
- Mix of secure and non-secure volumes
- Non-encrypting drives are used
- Secure and non-secure volumes on a single drive

Security Domains



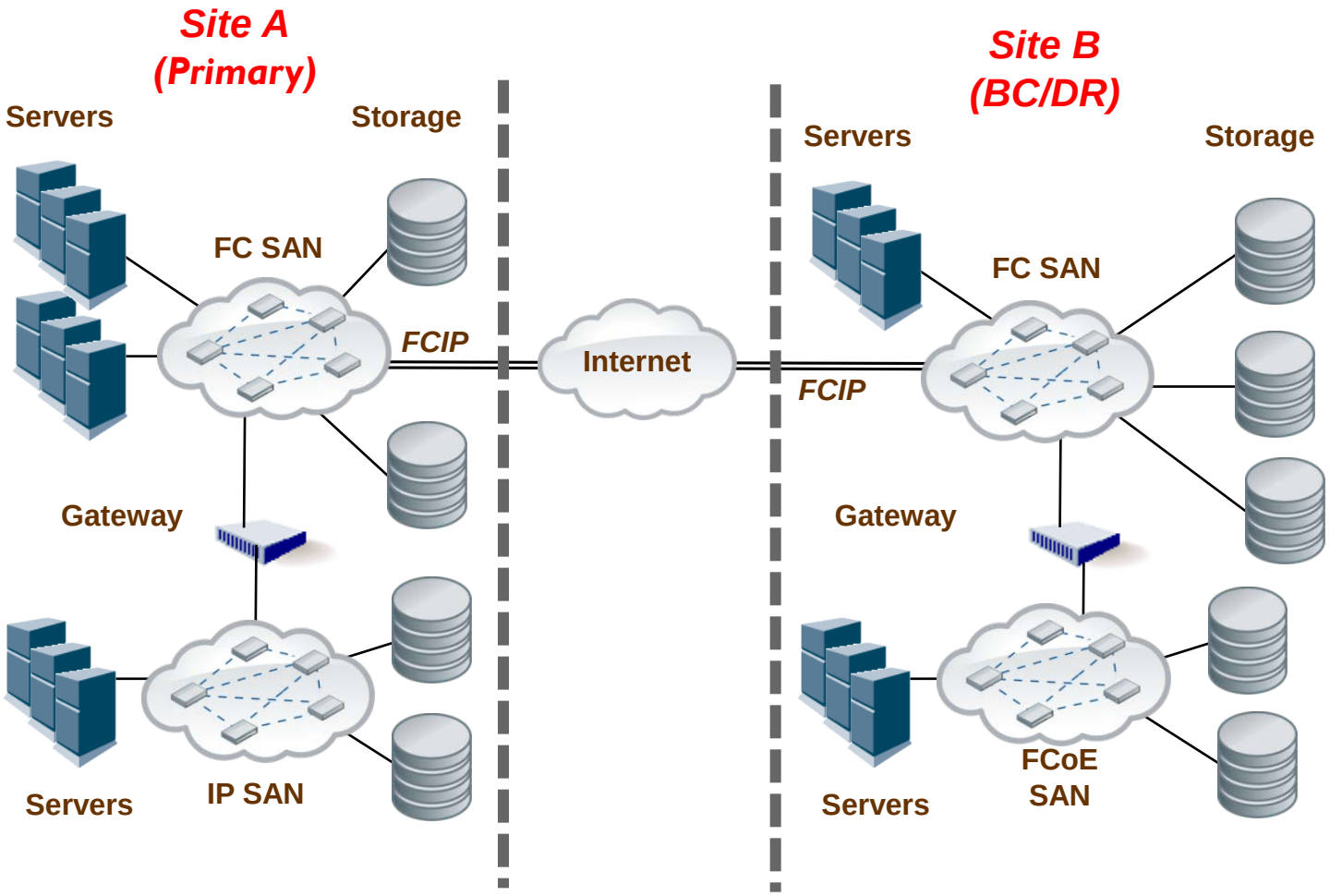
- Data must be secured across domain boundary
  - Electronic data
  - Physical data (tapes, drives, etc.)

Geographic Security Domains



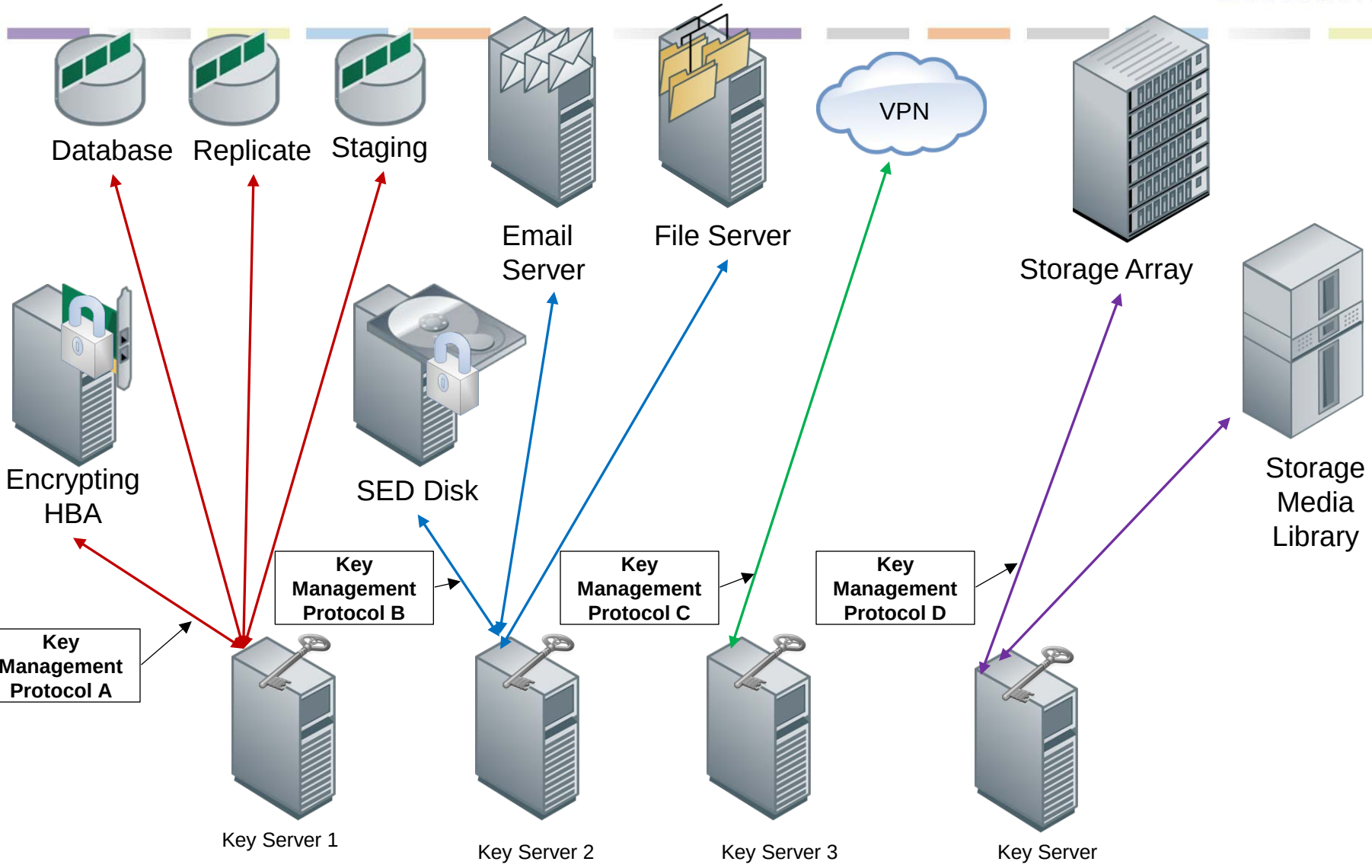
Source: ISO/IEC 27040 - Information technology - Security techniques - Storage security

Geographic Security Domains

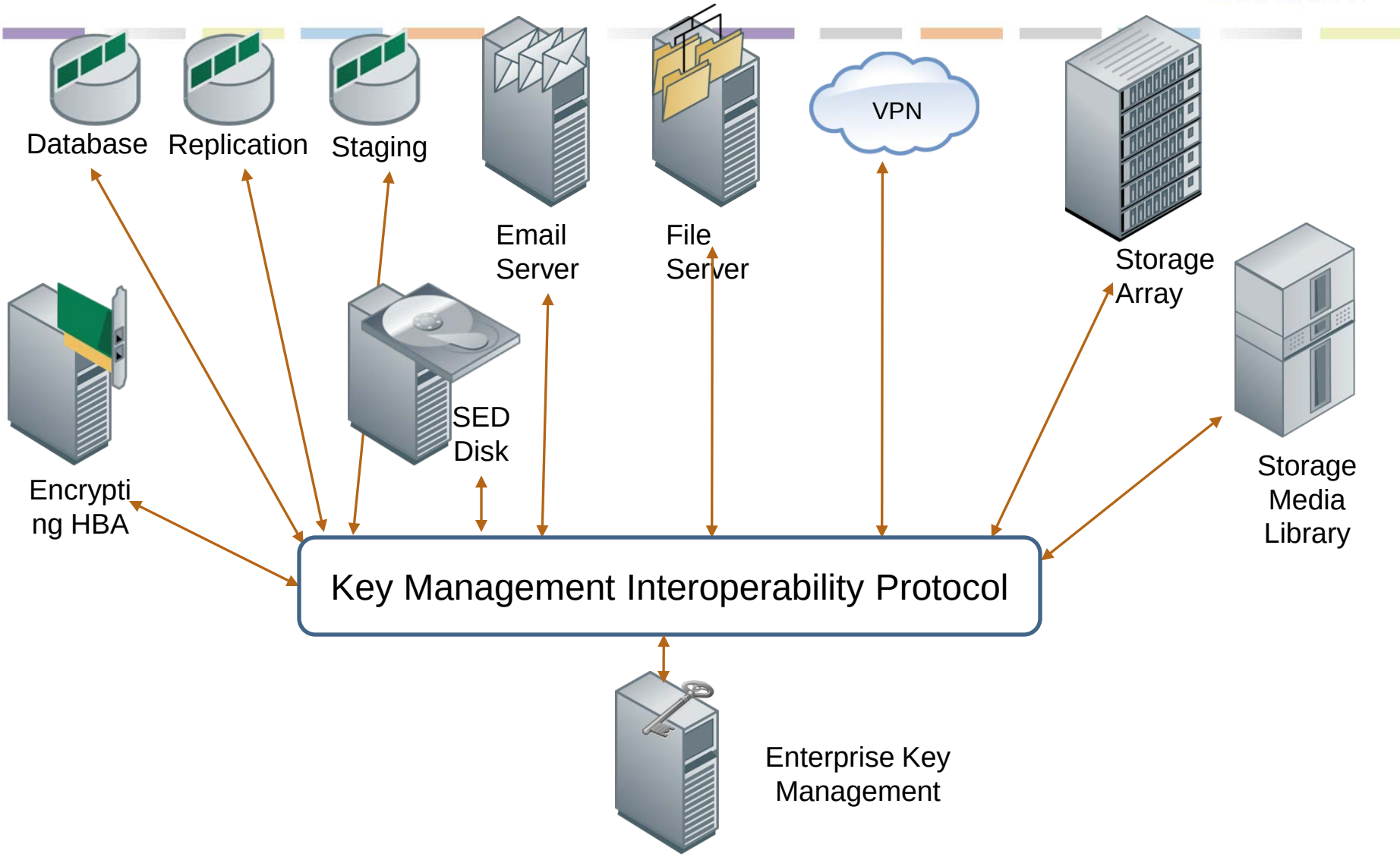


Source: ISO/IEC 27040 - Information technology - Security techniques - Storage security

Key Management



Standardized Key Management



Key Types

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

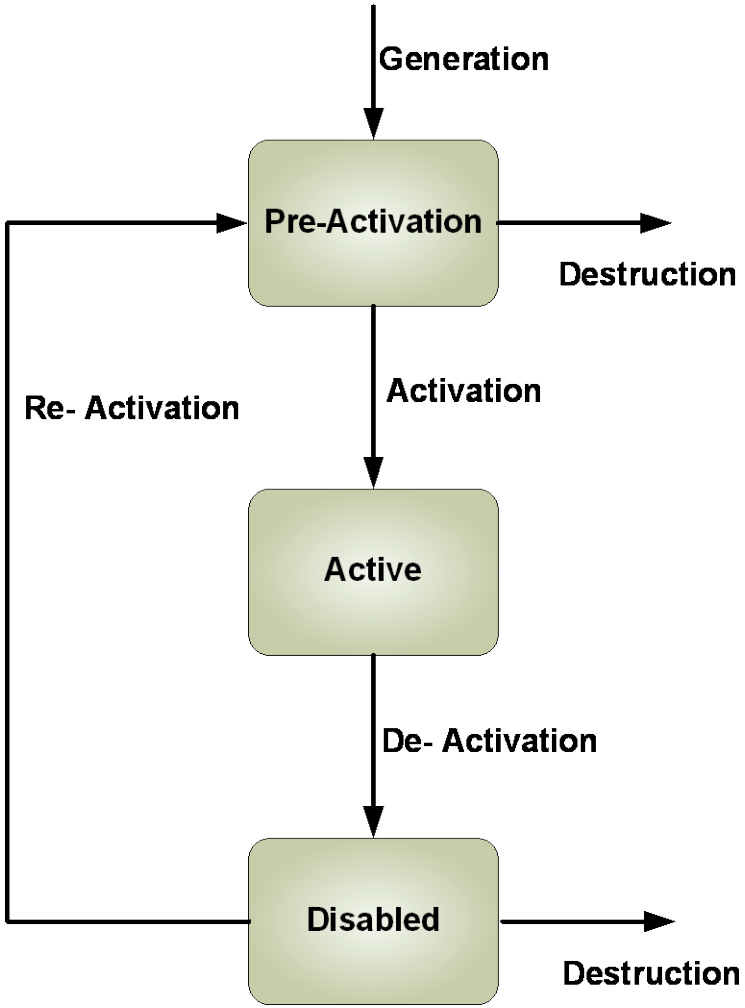
Key Uses

- Encryption Algorithms
  - AES
    - 128 Bit Key
    - 192 Bit Key
    - 256 Bit Key
  - 3DES
    - 168 Bit Key
- Encryption Algorithm Modes
  - Cipher Block Chaining Mode (CBC)
  - Cipher Feedback Mode (CFB)
  - Output Feedback Mode (OFB)
  - Counter Mode (CTR)
  - Galois/Counter Mode (GCM)
  - XOR-Encrypt-XOR (XEX)
  - XEX-TCB-CTS (XTS)
  - CBC-Mask-CBC (CMC)
  - ECB-Mask-ECB (EME)

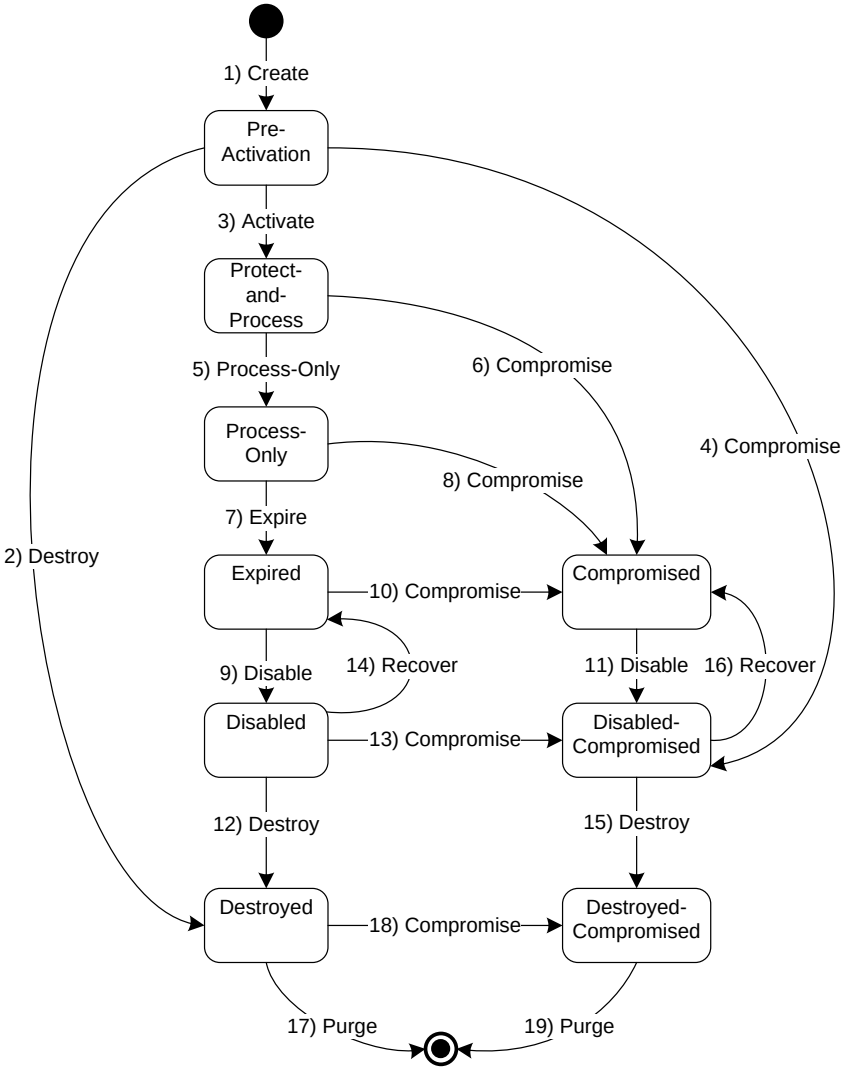
Key Management Issues

- Key management issues
  - Confidentiality
  - Integrity
  - Availability
  - Misuse
- Disclosure of key is disclosure of data
- Loss of key is doss of data
- Key availability is data availability

Key Lifecycle Overview



Real–Life Key Management



Source: IEEE P1619.3

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
- Keys need sufficient entropy
  - Enough randomness

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)
- SNIA: Audit Logging for Storage (http://www.snia.org/forums/ssif/knowledge_center/white_papers/forums/ssif/knowledge_center/white_papers/SNIA-Logging-WP.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)
- SNIA: Best Practices for Deploying a Storage Security Solution (http://www.snia-europe.org/news_events/e_news/)
- ISO/IEC 27040 — Information technology — Security techniques — Storage security (http://www.iso27001security.com/html/27040.html)

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)
- 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)
- IETF: Provisioning of Symmetric Keys (KEYPROV) (http://www.ietf.org/html.charters/keyprov-charter.html)

For More Information

- 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/
- Storage Security Industry Forum (SSIF)
  - Focus: Educational materials, customer needs, whitepapers, and best practices for storage security.
  - http://www.snia.org/ssif

For More Information

Check out SNIA Tutorials:

https://www.snia.org/education/tutorials/security

- **Introduction to Key Management for Secure Storage**
- **An Inside Look at Imminent Key Management Standards**
- **Introduction to Storage Security**
- **Legal Issues Relevant to Storage**
- **And More!**

Q&A / Feedback

- Please send any questions or comments on this presentation to SNIA: www.tracktutorials@snia.org

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

- SNIA Education Committee

Larry Hofer CISSP	**SNIA SSIF**
Eric Hibbard CISSP	**SNIA Security TWG**
Richard Austin	**Roger Cummings**
Gianna DaGiau	**Michael Willett**