
Education

# An Introduction to Key Management for Secure Storage

Walt Hubis, LSI Corporation

# SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA.
- 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


## An Introduction to Key Management for Secure Storage

As secure storage becomes more pervasive throughout the enterprise, the focus quickly moves from implementing encrypting storage devices to establishing effective key management policies. Without the proper generation, distribution, storage, and recovery of key material, valuable data will be eventually compromised. Worse, without proper management of key information, data can be completely lost.

This session explores the fundamental issues and technologies that impact key management for disk, tape, array, and other storage devices. Major issues associated with symmetric encryption keys are presented, along with practical advice on effective key management practices.

# The Key Management Problem

# The Key Management Problem

# The Key Management Problem

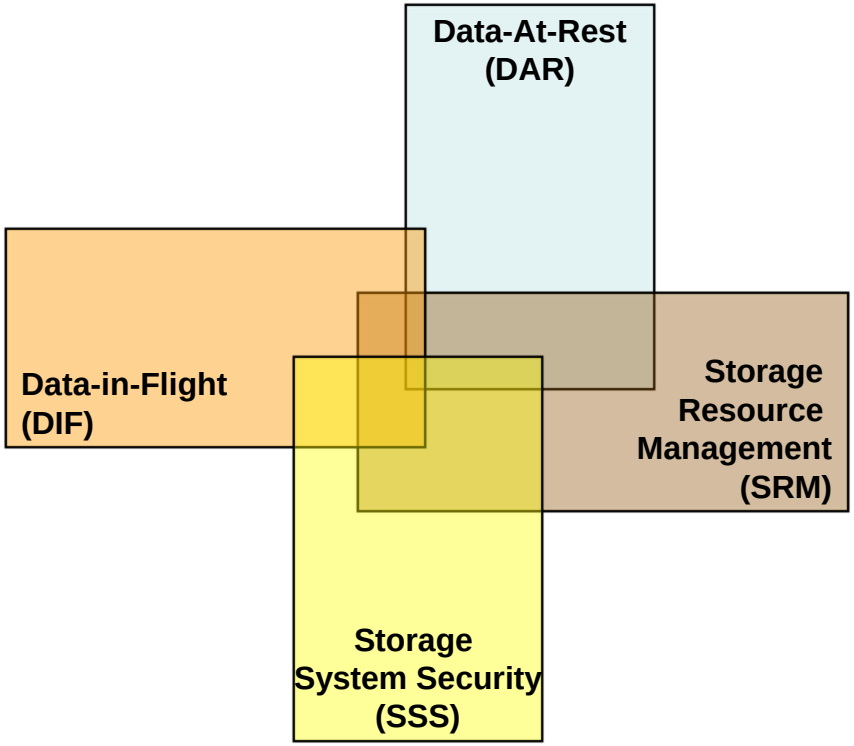
# Data At Rest

- Random Access Devices
  - Disk Drives
- Sequential Access Devices
  - Tape Drives
- Other Media
  - Optical Media
- Data in Flight is Still Important!

**Check out SNIA Tutorial:**

**Self-Encrypting Storage**

# Data At Rest




| Storage Element | Description |
|---|---|
| Data-At-Rest (DAR) | "Protecting the confidentiality, integrity and/or availability of data residing on servers, storage arrays, NAS appliances and other media" |
| Storage Resource Management (SRM) | "Securely provisioning, monitoring, tuning, reallocation, and controlling the storage resources so that data may be stored and retrieved." |
| Storage System Security (SSS) | "Securing embedded operating systems and applications as well as integration with IT and security infrastructure (e.g., external authentication services, centralized logging and firewalls" |
| Data-in-Flight (DIF) | "Protecting the confidentiality, integrity and/or availability of data as they are transferred across the storage network, the LAN, and the WAN. Also applies to management traffic" |

Source: Introduction to Storage Security, A SNIA Security Whitepaper, September 9, 2009

# 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

# Key Management

- 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

- Key and Data Lifetime
  - Forever
    - Assure Access to Data Years from Now
  - For a Limited Time Period
    - Ephemeral – Milliseconds, Seconds
    - Weeks, Months, Years
- What Happens at End of Life?
  - Mandatory Re-Encryption
  - Destruction of Data
  - Destruction of Key

# Key Management

- Policies
  - Who Can Establish Keys?
  - Who Can Delete Keys?
  - What is the Lifetime of a Key?
  - Can the Key be Archived?
  - Are the Keys Changed Periodically?
  - Are Keys Automatically Deleted or Archived?
  - Who Else Can Use the Key?

# Key Management

- Auditing
  - Track the Key over it's Lifetime
  - Who Created the Key and When?
  - Who Changed the Key and When?
  - Who Created a Copy of the Key and When?
  - Where are the Copies of the Key
  - Who Deleted the Key and When?

# Key Management

- Threats
  - Confidentiality
    - Key Disclosure
    - Data Accessible to Anyone
  - Integrity
    - Key has Been Modified
    - Key has been Corrupted
    - Data Accessible by None
  - Archive
    - Key has Been Lost
  - Availability
    - Key Cannot be Accessed

# Key Management Goals

- Backup/Restore Key Material
- Archival and Retention of Key Material
- Distribution of Key Material
- Expiration, Deletion, and Destruction of Key Material
- Audit of Key's Life Cycle
- Reporting Events and Alerts

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

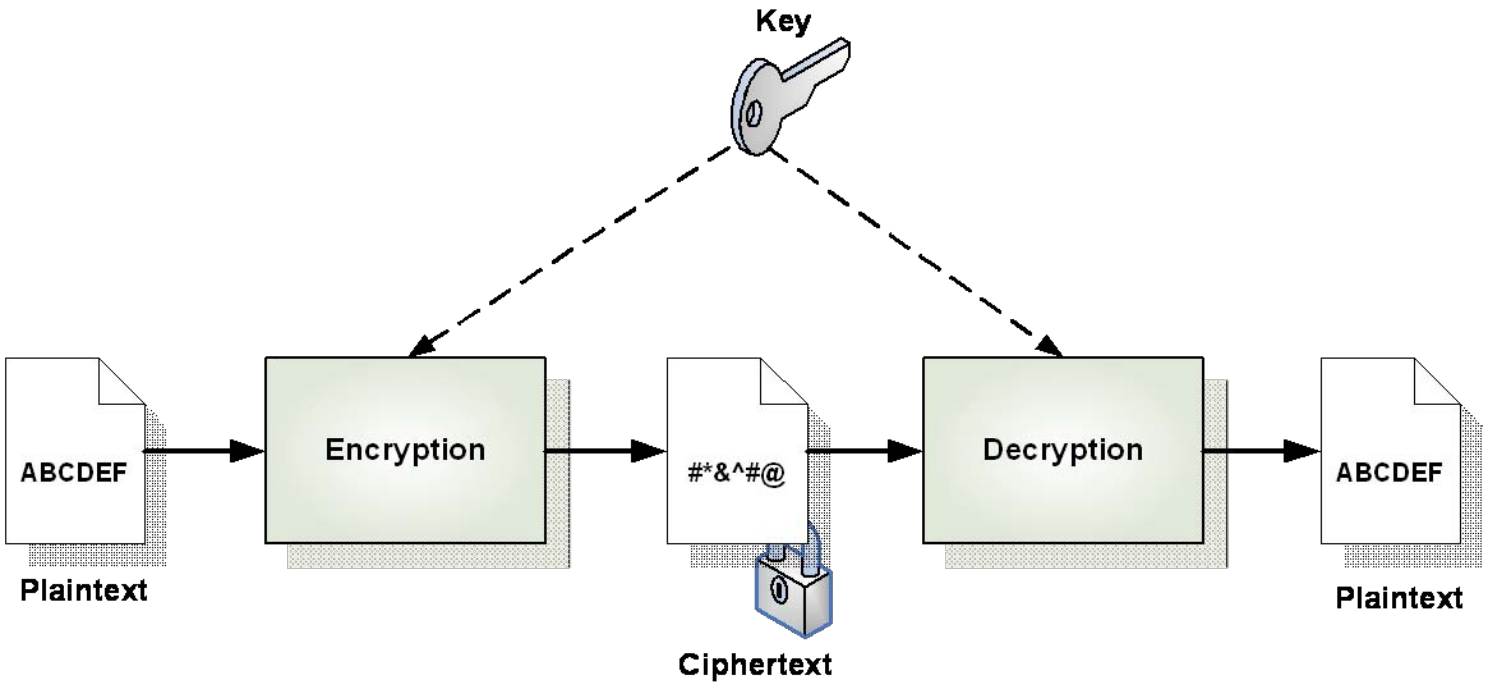
# Keying Material

# Keys

- Two Major Types of Encryption
  - Symmetric Keys
  - Asymmetric Keys
- Storage Systems May Use Both
  - Asymmetric Keys to Exchange Symmetric Keys
  - Symmetric Keys to Encrypt/Decrypt Data

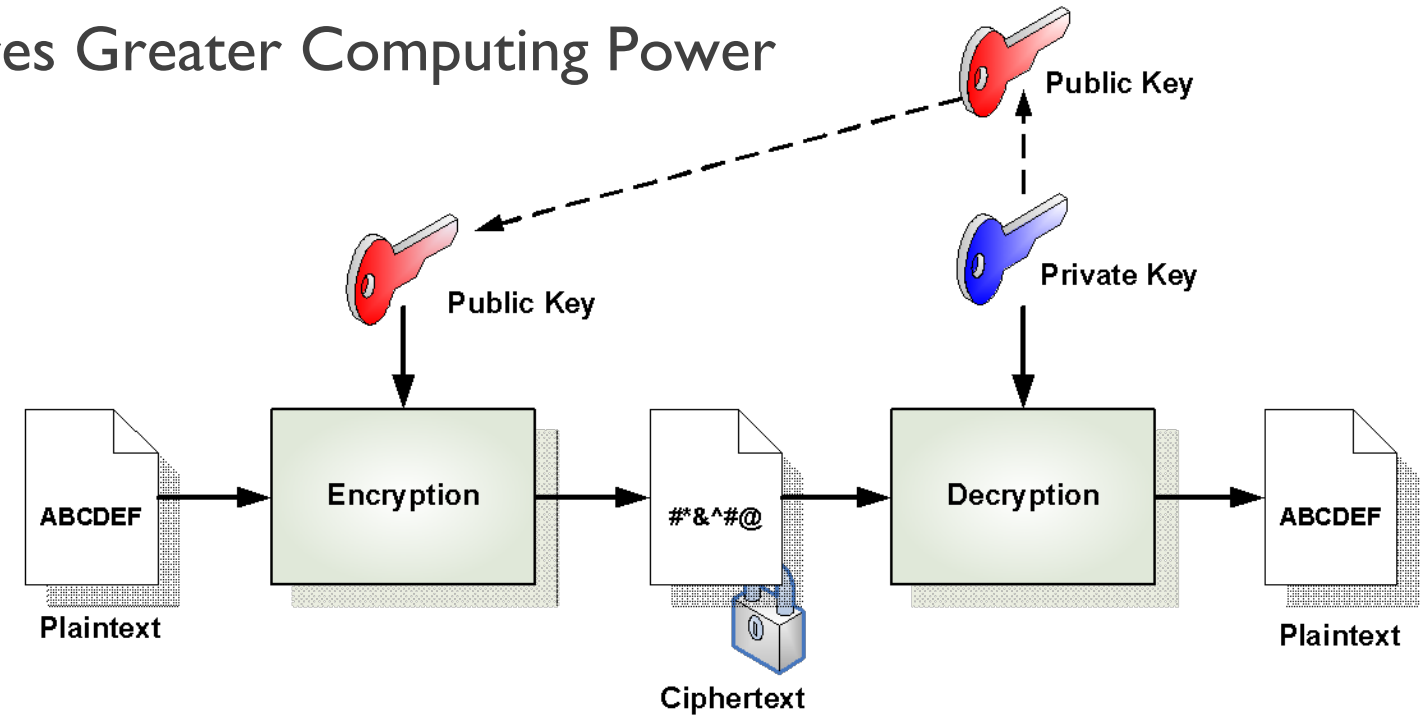
# Symmetric Keys

- One Key
  - Used for Both Encryption and Decryption
- Requires Lower Computing Power

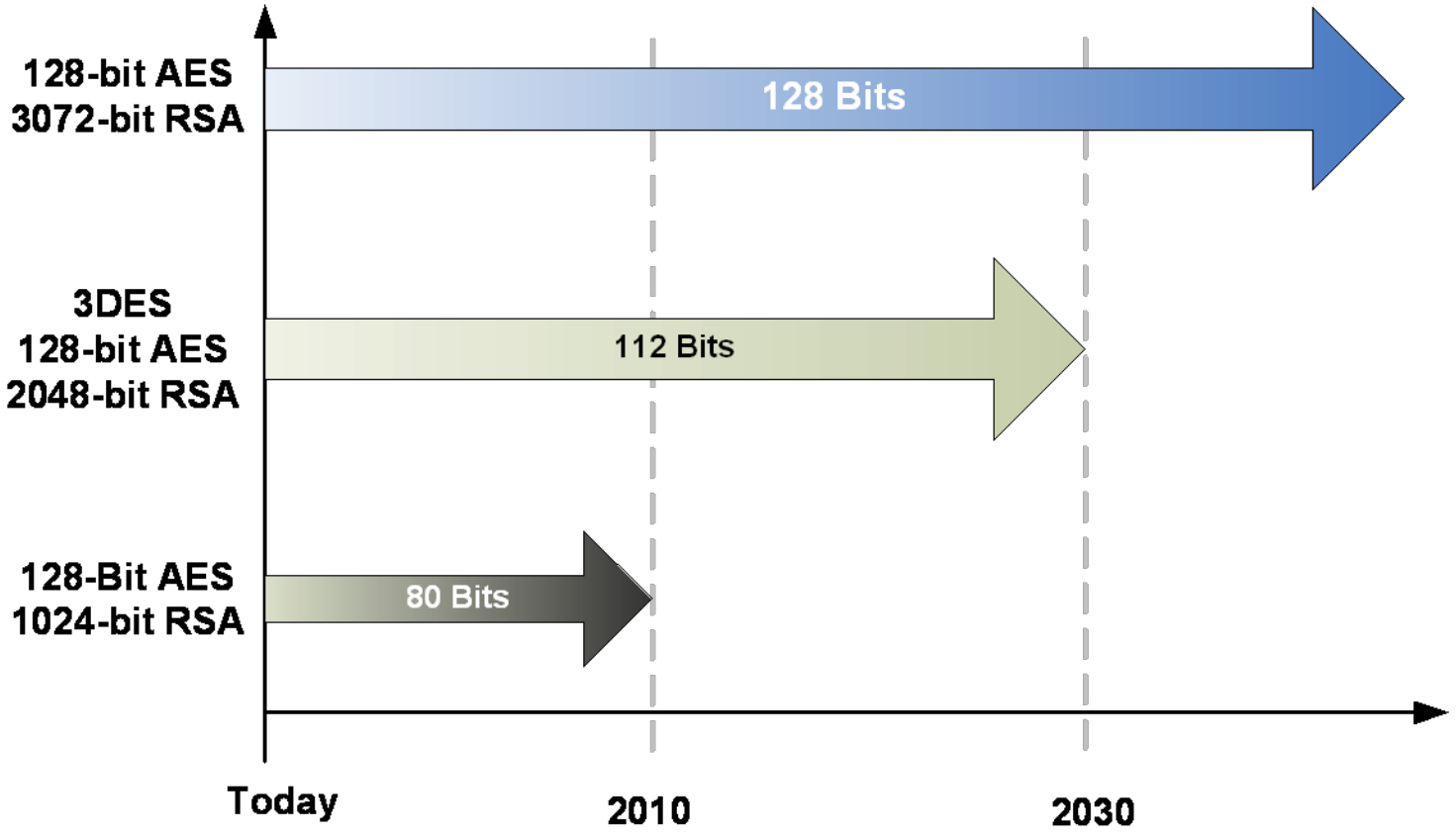


# Asymmetric Key

- Uses Private and Public Key Pair
  - Can't be Derived from Each Other
  - Data Encrypted with One Can Only Be Decrypted With the Other
  - Requires Greater Computing Power



# Encryption Strength

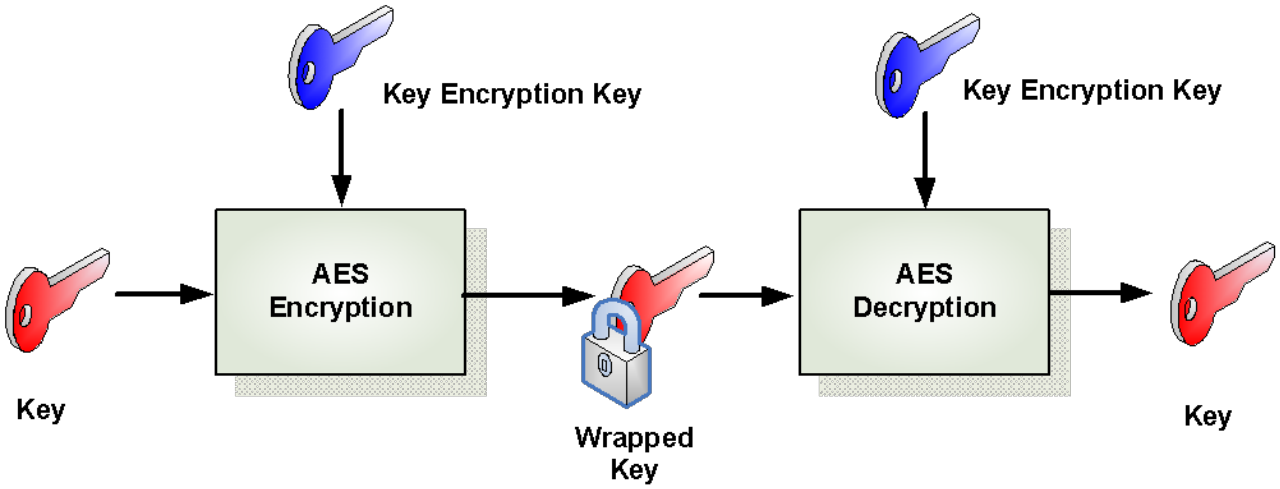


# Key Formats

- Key Formats
  - Any and All Key Formats Must Be Managed
  - Keys are Viewed as Objects
- Key Material
  - Key Data
  - Key Information: Metadata
- Storage Generally Uses Symmetric Keys
  - A Secure Key Exchange Assumed
  - Easier to Implement
  - Less Client Resources

# Key Wrapping

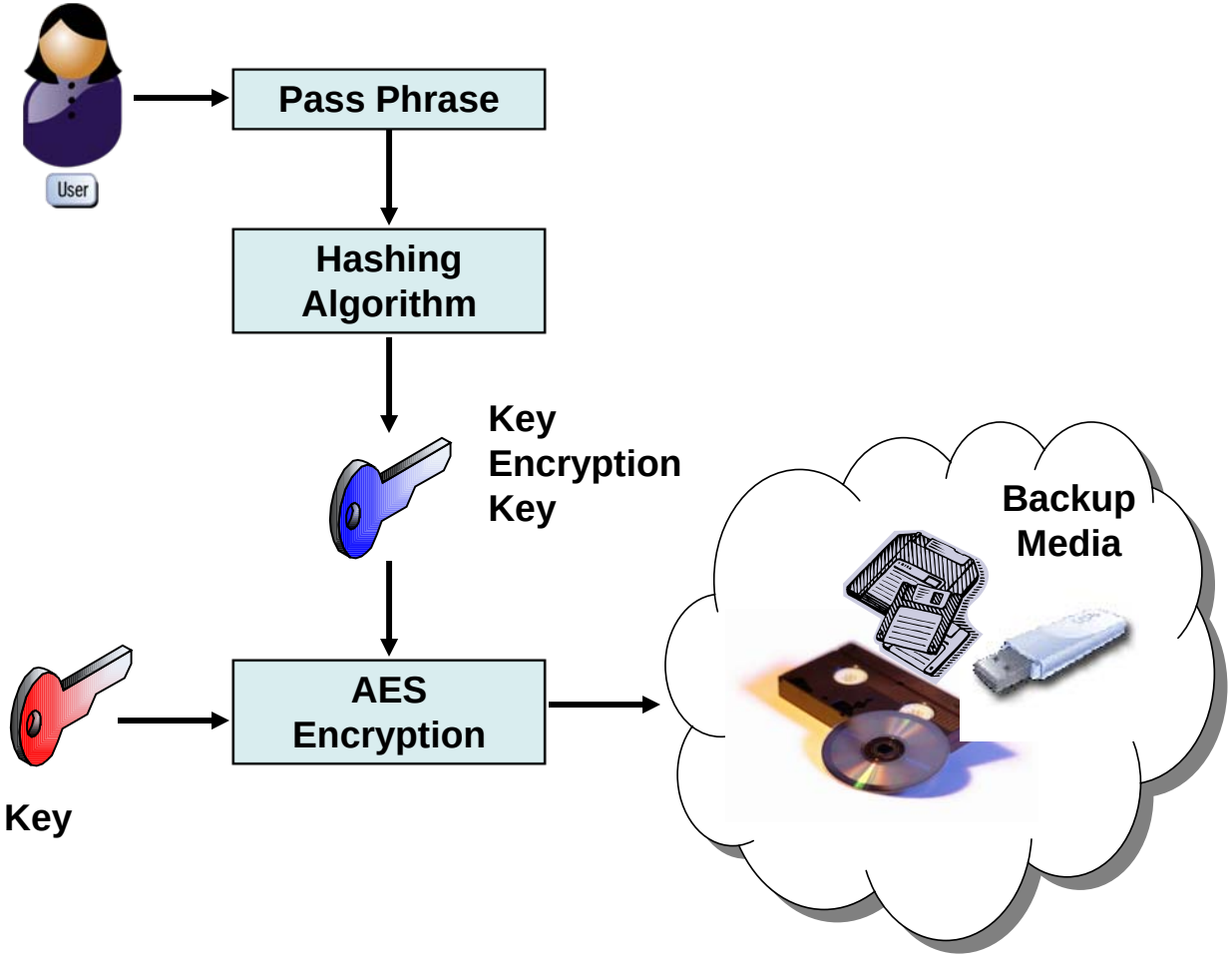
- Used to Move Keys
  - Backup
  - Archiving
  - Installation




Source: AES Key Wrap Specification (http://csrc.nist.gov/CryptoToolkit/kms/key-wrap.pdf)

# Pass Phrase

- Commonly Used to Generate Key Encryption Key



# Basic Key Metadata

- Value
  - The Actual Key
- Unique Identifier (GUID)
  - Unique Within a  Domain (Name Space)
    - The Domain May be World Wide Unique
  - May be a Globally Unique Identifier
    - World Wide Unique Name
  - May be a Hierarchy
  - Important for Identifying Keys that are Moved
    - Across Domains
    - Across Companies
    - Across Countries

# Optional Key Metadata

- Name
  - User readable name, not necessarily Unique
- Creator name
- Domain name
- Parent GUID
- Previous version GUID
- Version string

# Optional Key Metadata

- Timestamps
  - Creation
  - Modified
  - Valid Time
  - Expiration Time
- Policies
  - Use of key
  - Key type
- Access rights - who can:
  - Access
  - Modify
  - Disable
  - Destroy
- Vendor-Specific Metadata

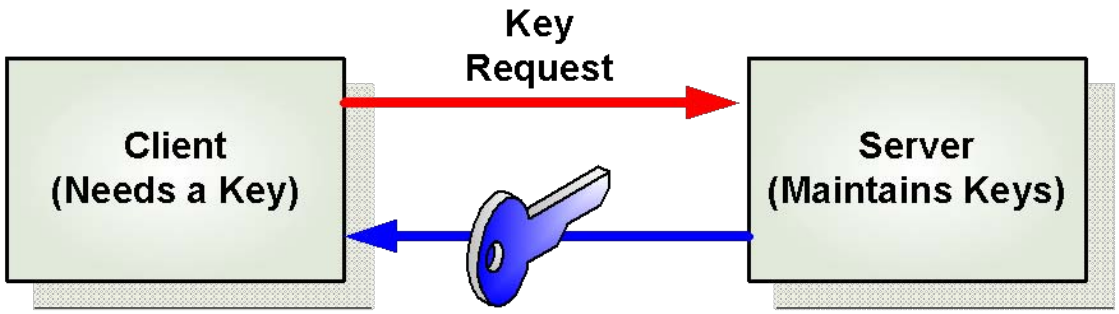
# Key Management Components

# Key Management Components

- Client-Server View
- The Key
- The Key Server
- The Key Transport Channel
  - Secure Channel
  - Authentication
  - In-Band
  - Out of Band
- Key Exchange Protocol

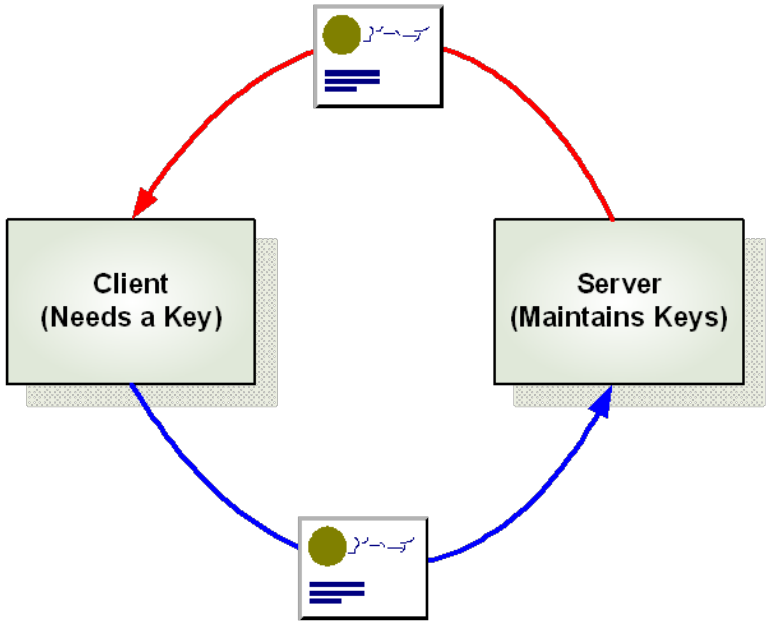
# Client-Server View

- Client
  - User or Consumer of Keys
- Server
  - Provider of Keys



# Client-Server Authentication

- Client and Server Must Authenticate
  - Assures Identity
  - Secrets or Certificates
  - Pre-Shared Keys or PKI
- Communications are Secure
  - Channel Encryption



# Key Clients - Lightweight

- Limited Resources
  - Limited Computational Requirements
  - Limited Memory Requirements
- Applications
  - Disk Drives
  - Tape Drives, Libraries
  - Array Controllers
- Simple Protocol
  - Fixed Fields and Values
  - Similar to SCSI CDBs

# Key Clients - Complex

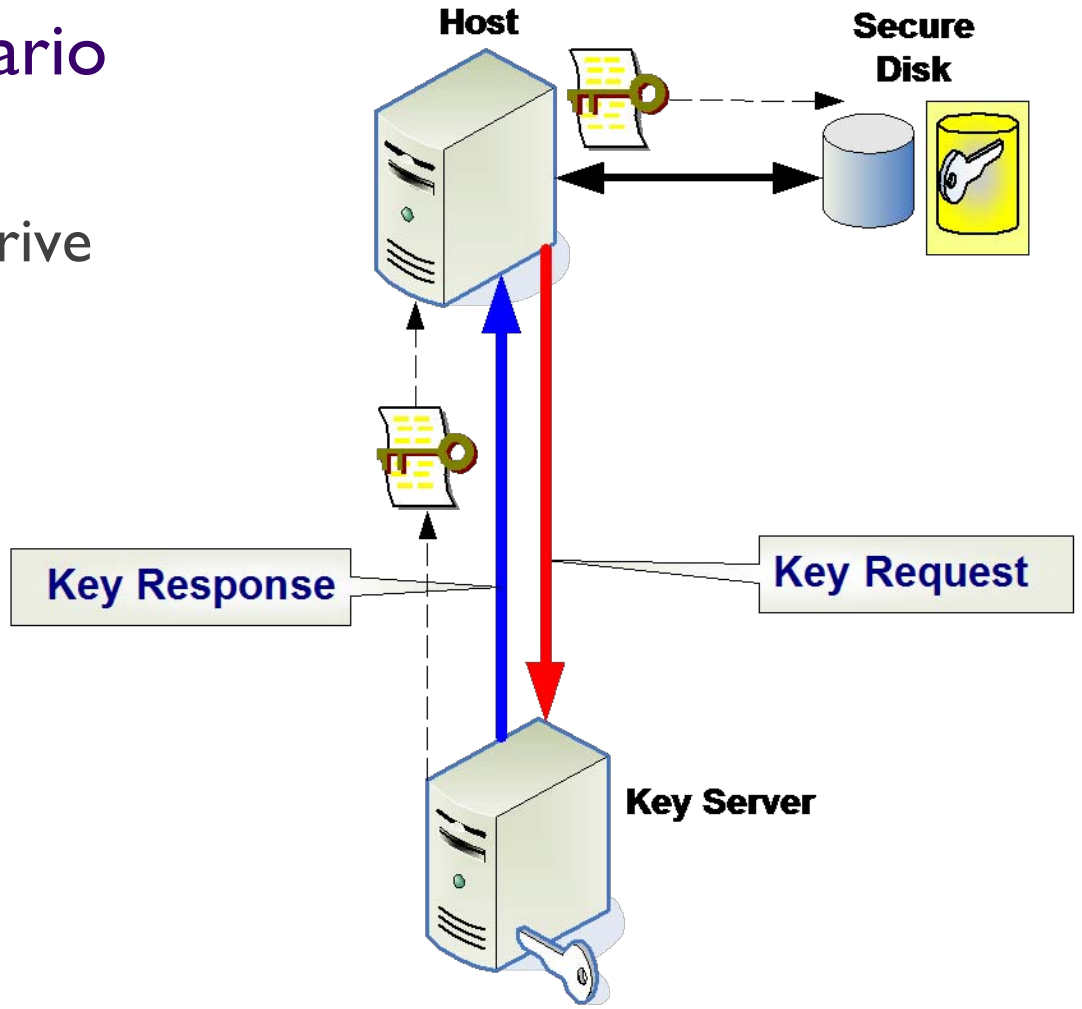
- Unlimited Resources
- Applications
  - Key Servers
  - Data Bases
  - Objects
  - File Servers
- May Use a Complex Protocol
  - Requires Complex Protocol Parser

# Key Server

- Key Server
  - Software Application
    - Generic Hardware Platform
  - Dedicated Hardware Servers
    - Hardened
- Multiple Key Servers
  - Key Management Between Servers
- Policy Management
  - Accounting
  - Validation
- Backup

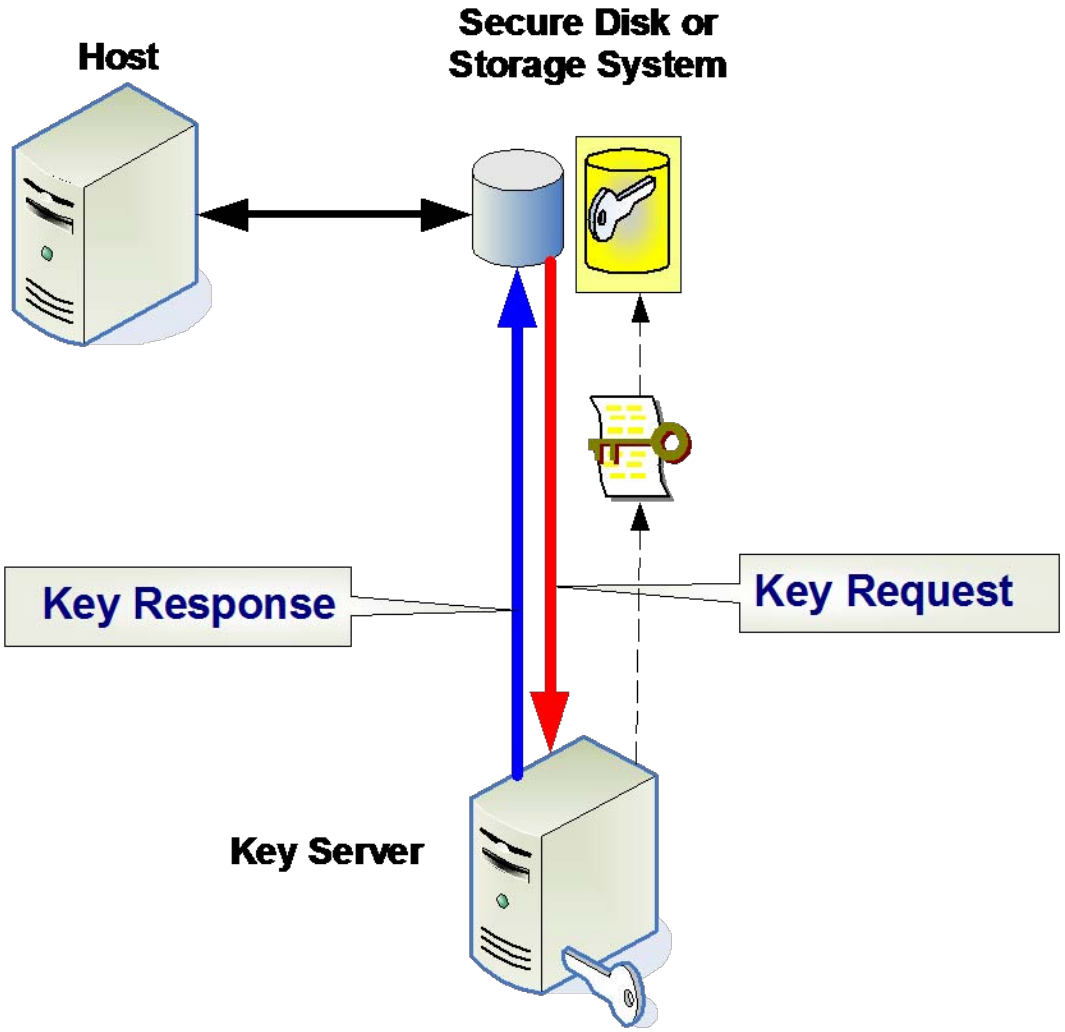
# Key Clients and Servers - Disk

- Typical KM Scenario
  - Client: Host PC
  - Passes Key to Drive



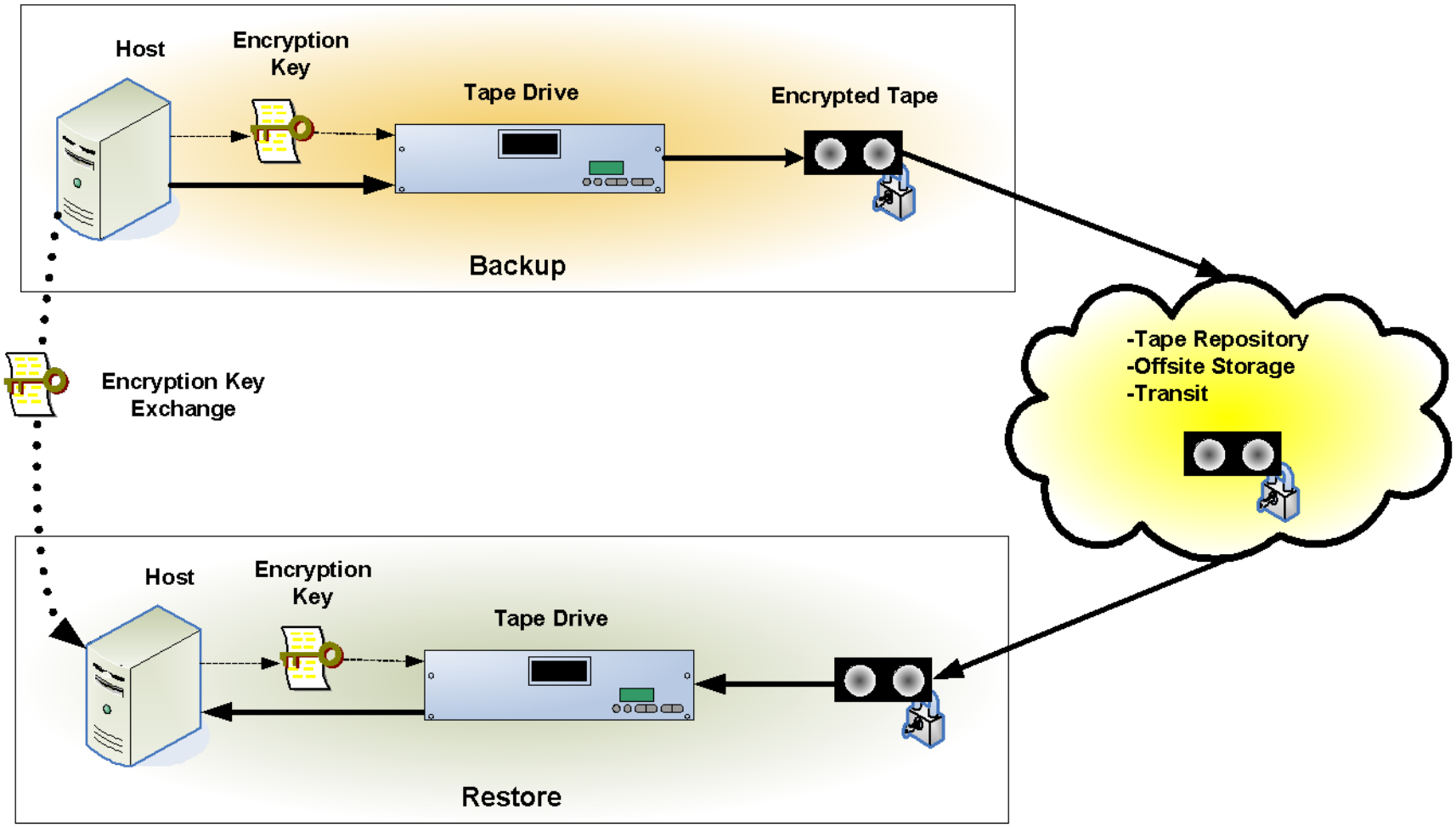
# Key Clients and Servers - Disk

- Client is the Drive
  - Drive or Subsystem
  - Requests Key Directly from Server



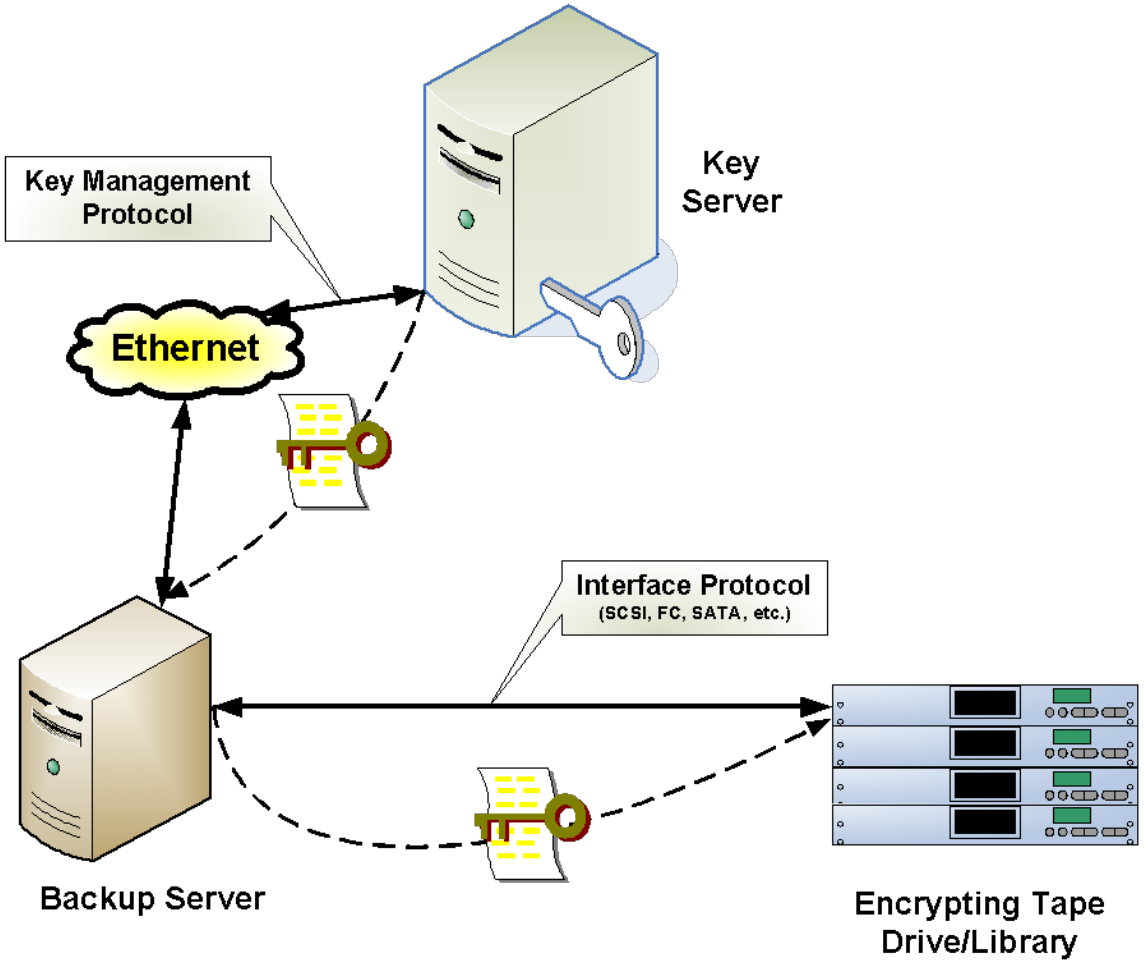
# Key Clients and Servers - Tape

## Manual Key Management



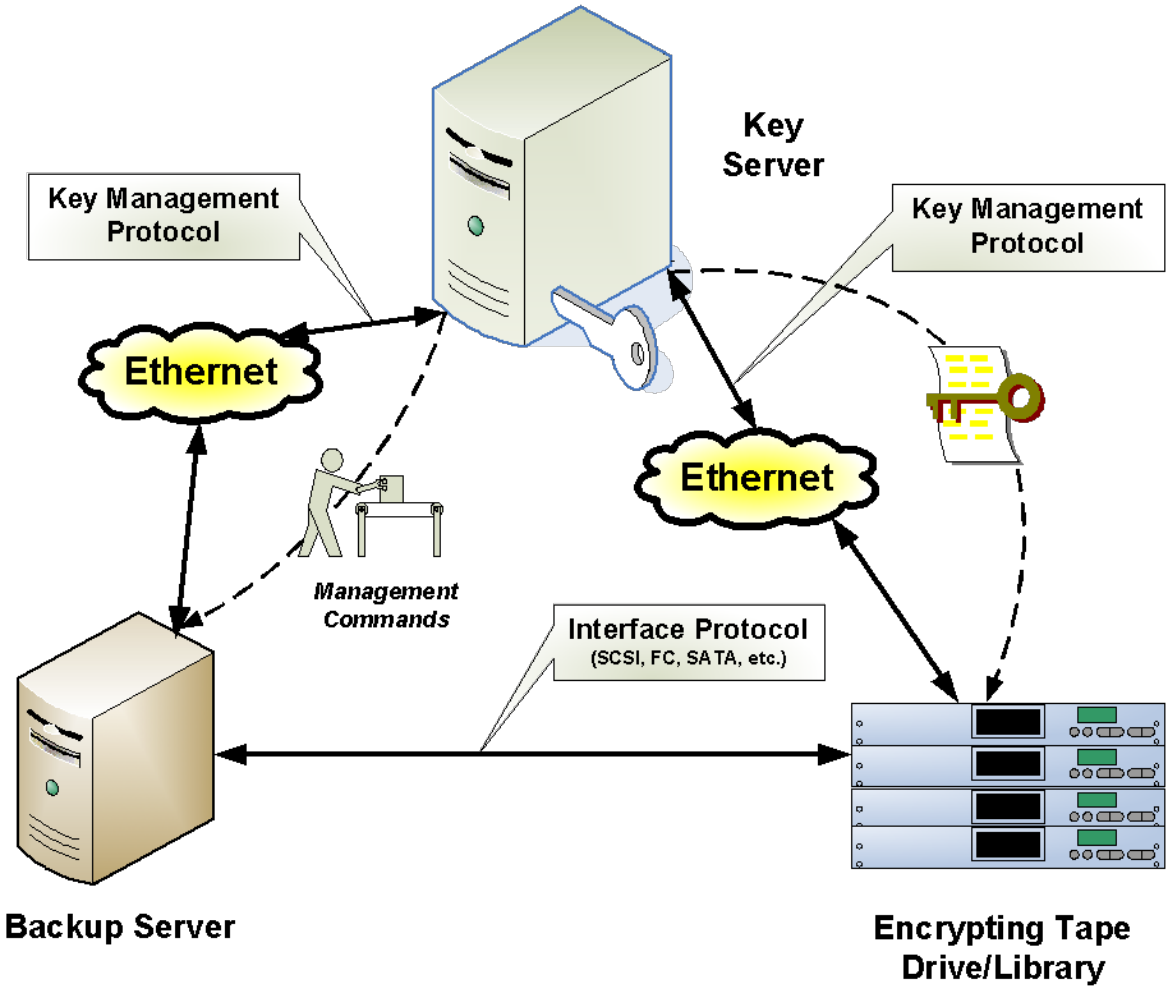
# Key Clients and Servers - Tape

- Automated Key Management



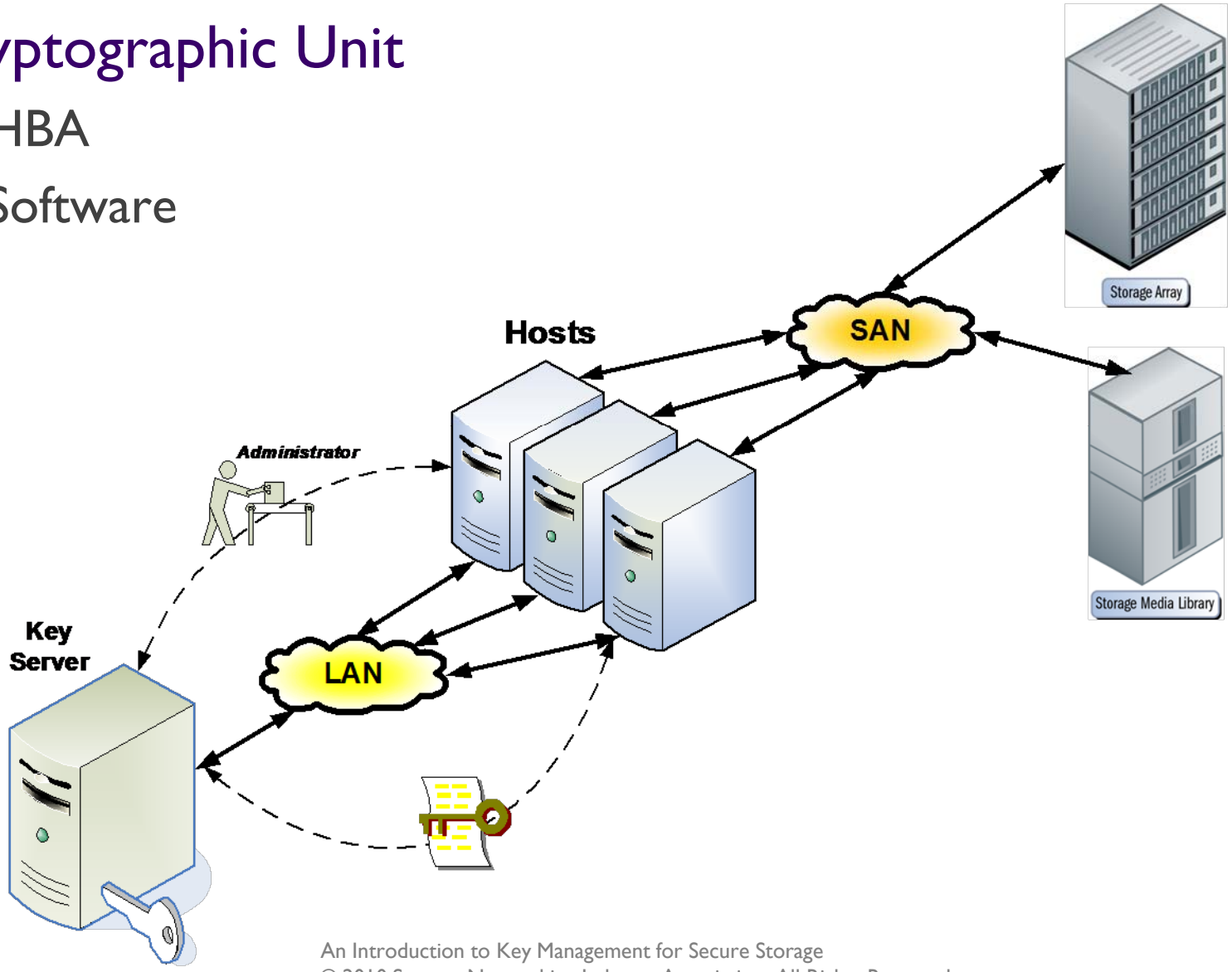
# Key Clients and Servers - Tape

- Automated Key Management

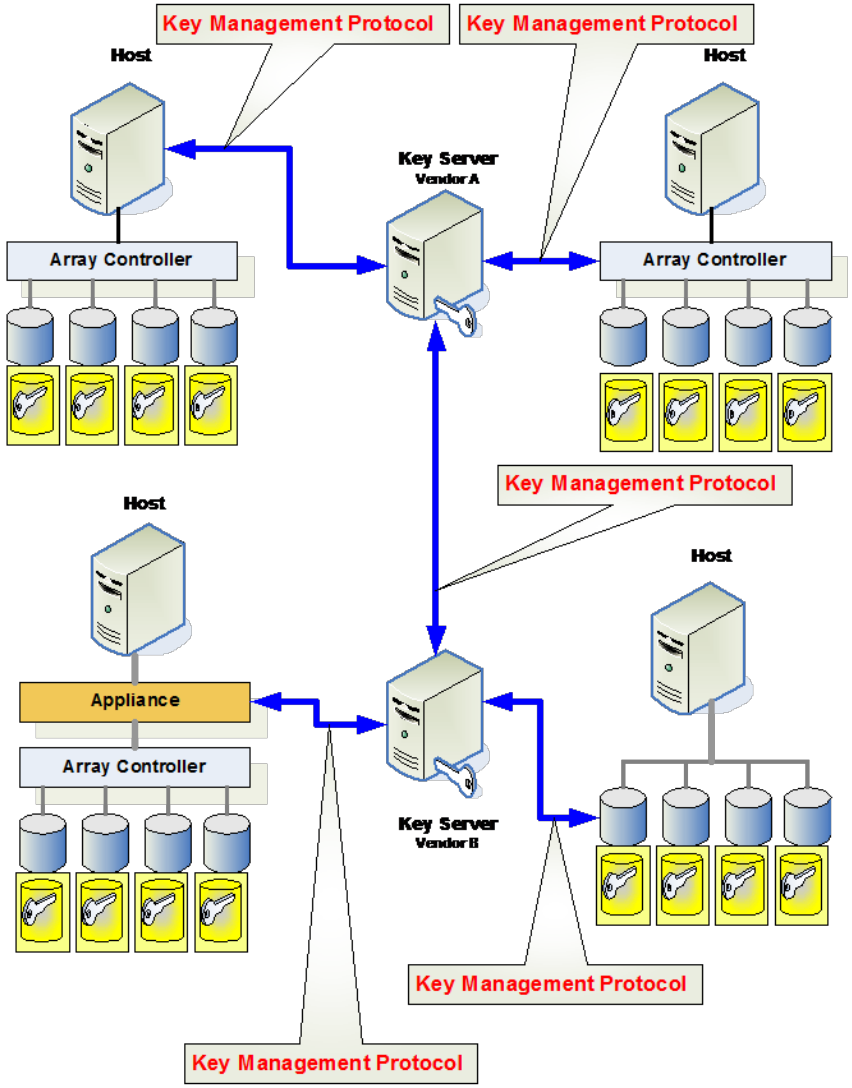


# Host Based Key Management

- Cryptographic Unit
  - HBA
  - Software



# Key Clients and Servers - Enterprise

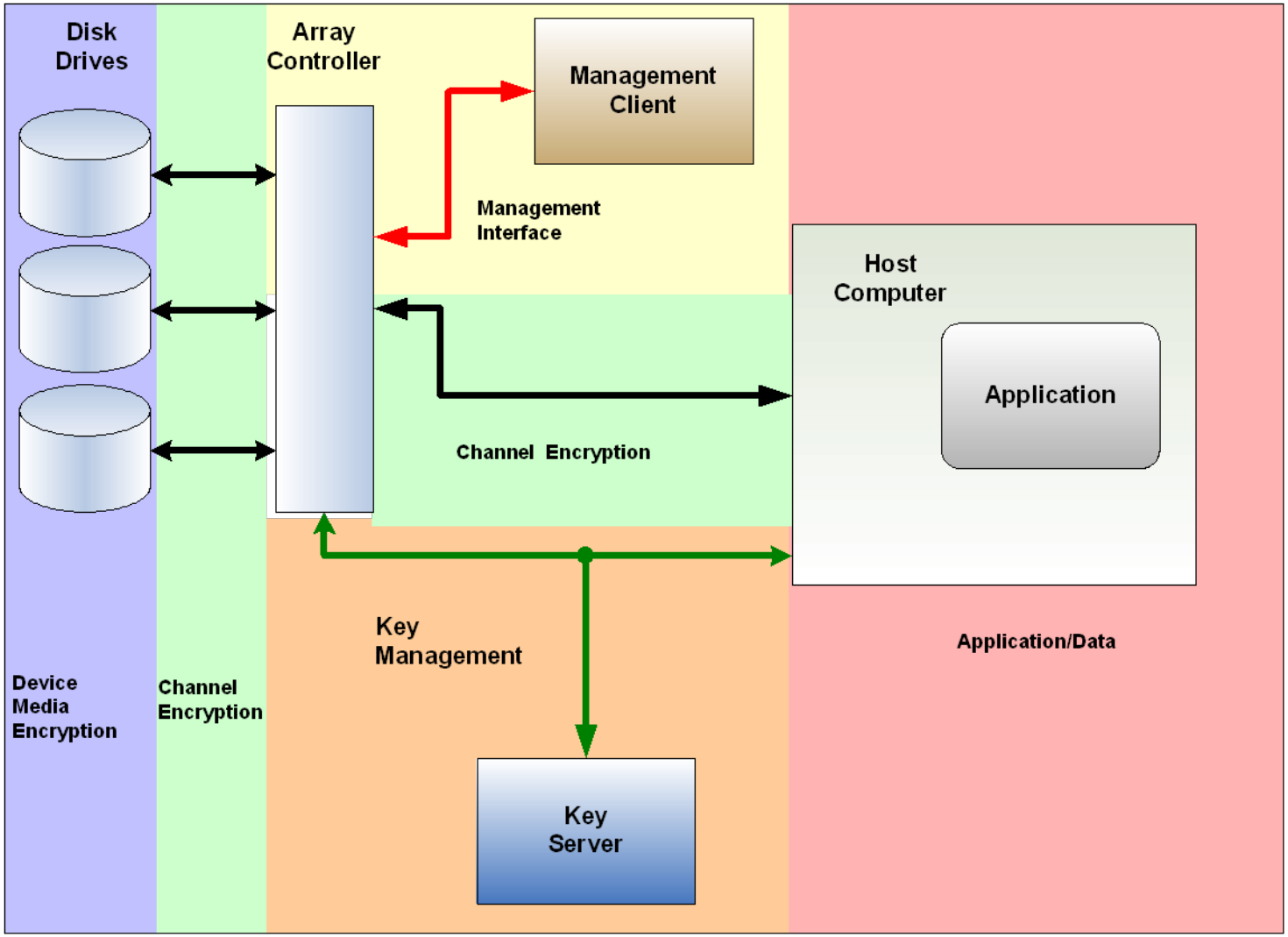


# KMS Protocol

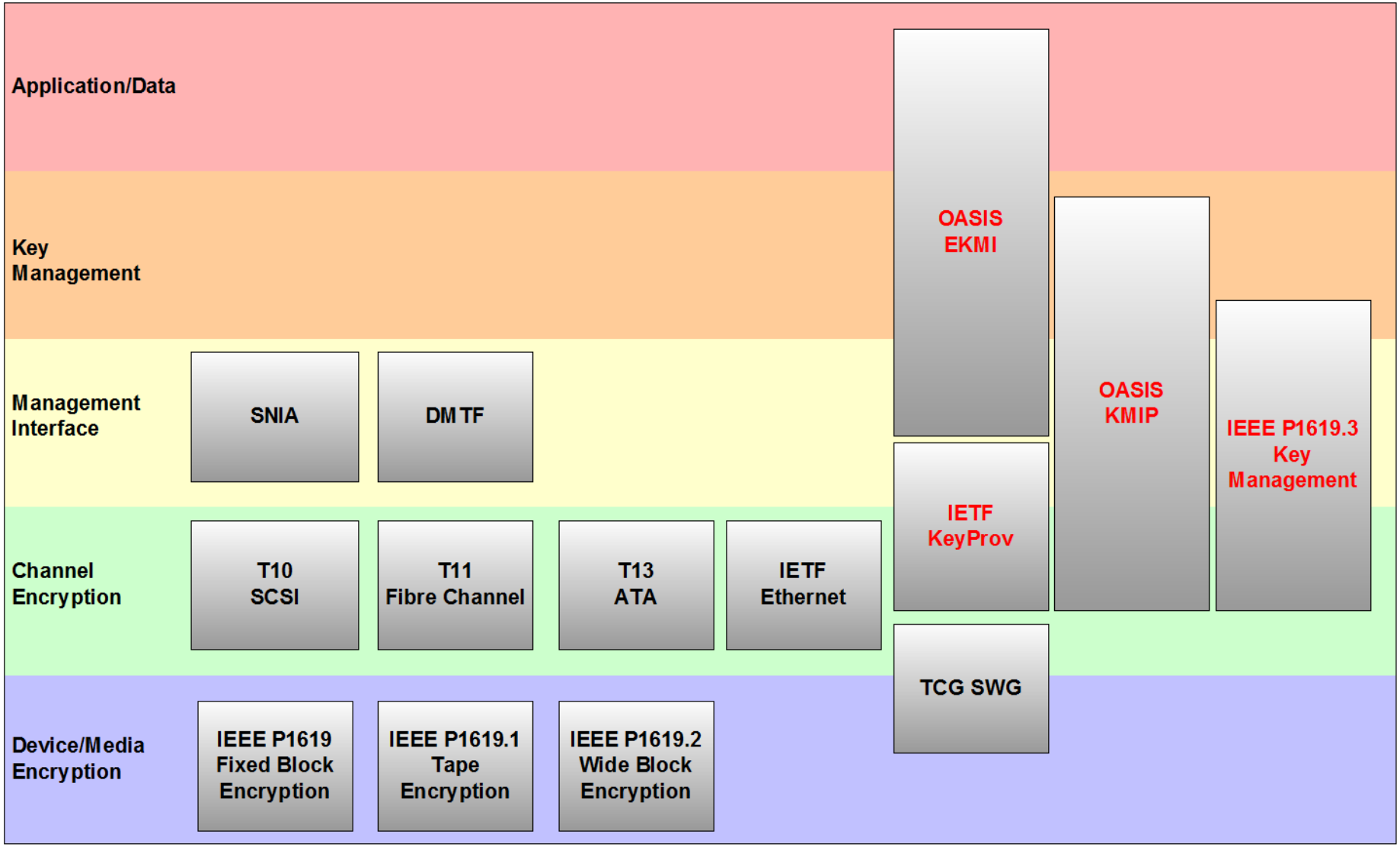
- Two Primary Operations
  - Set key
    - Server ⇨Client
  - Get key
    - Client ⇦Server
- Optional Operations
  - Find key
  - Update key
  - Replicate key
  - Disable key
  - Destroy key
  - Access rights
  - Get service info
  - Audit log functions

# Key Management Standards for Storage

# Key Management Standards for Storage



# Key Management Standards for Storage



# For More Information

**Check out SNIA Tutorial:**

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

# 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)

# Q&A / Feedback

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

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

*SNIA Education Committee*

Larry Hofer CISSP
Eric Hibbard CISSP
Mark Nossokoff
Blair Semple
SNIA SSIF
SNIA Security TWG