Key Management

The Key to Secure Storage

Michael Willett

Seagate Technology

Trusted Computing Group

© 2008 Insert Copyright Information Here. All Rights Reserved.

Overview

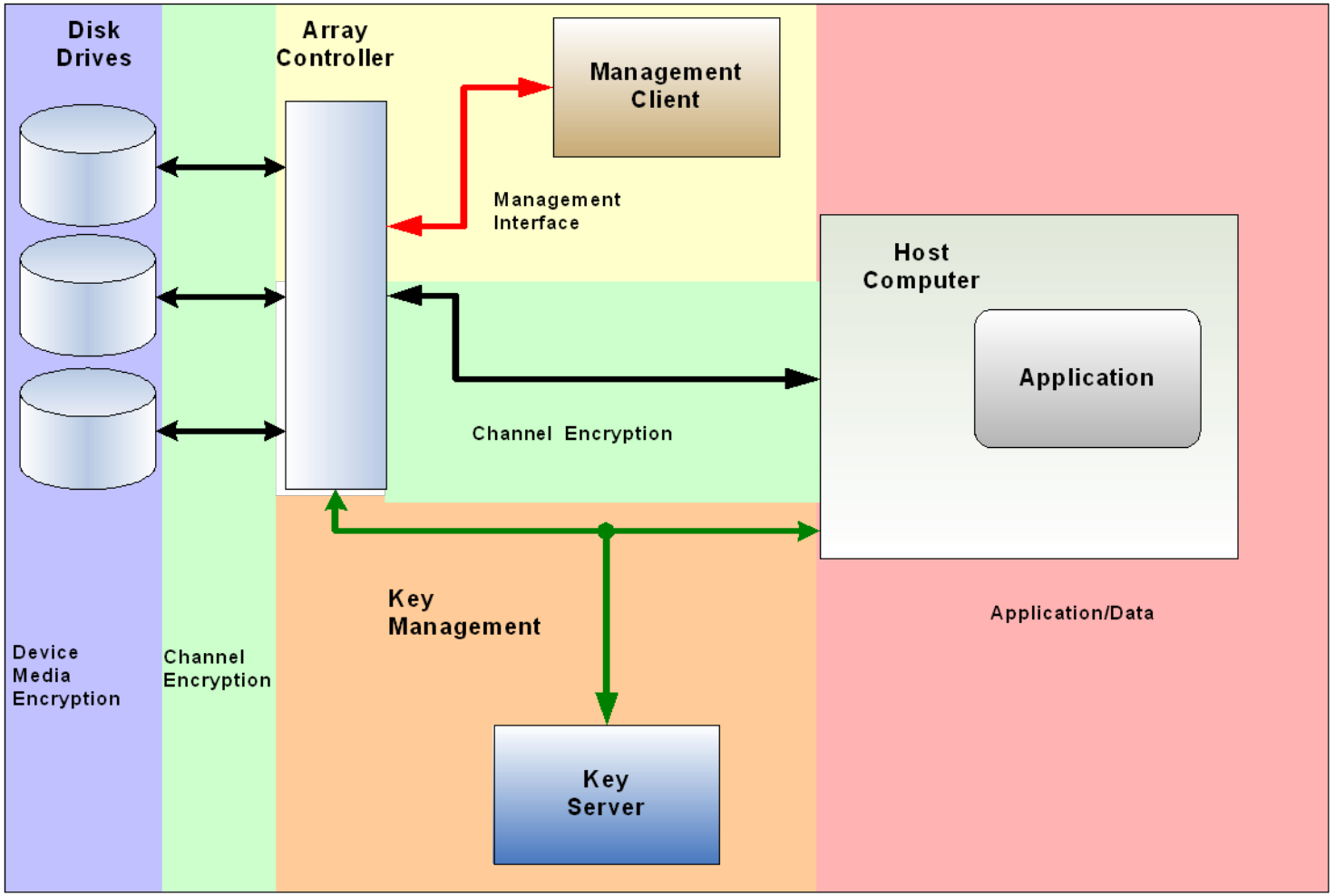
- Basic Key Types
- Uses of Keys
- Key Management
- Standards Organizations

© 2008 Insert Copyright Information Here. All Rights Reserved.

Keys

© 2008 Insert Copyright Information Here. All Rights Reserved.

Key Usage



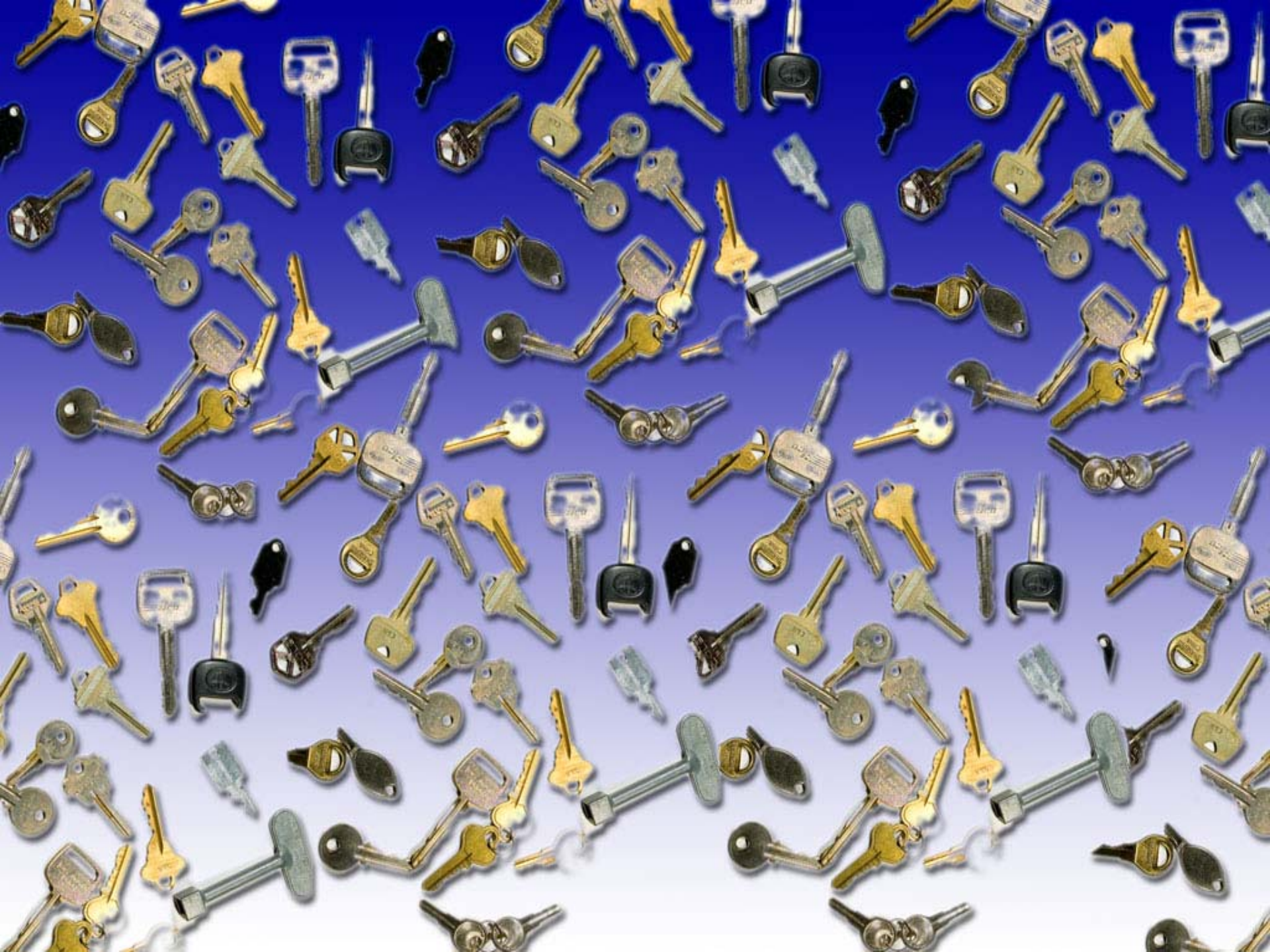
© 2008 Insert Copyright Information Here. All Rights Reserved.

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

- 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

© 2008 Insert Copyright Information Here. All Rights Reserved.



Basic Key Types

- Data Encryption Keys
  - Symmetric Keys
  - Long Key Lifetime
  - Loss of Key is Loss Of Data
  - Secure Erase
  - Audits

© 2008 Insert Copyright Information Here. All Rights Reserved.

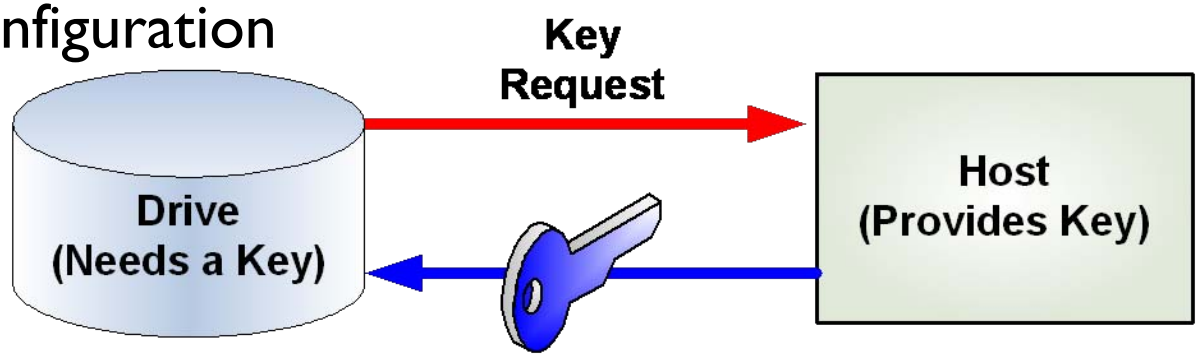
Basic Key Types

- Key Encryption Keys
  - Used to Securely Transfer Data Encryption Keys
  - Ephemeral
  - Asymmetric: Public Key Infrastructure (PKI)

© 2008 Insert Copyright Information Here. All Rights Reserved.

Access Key

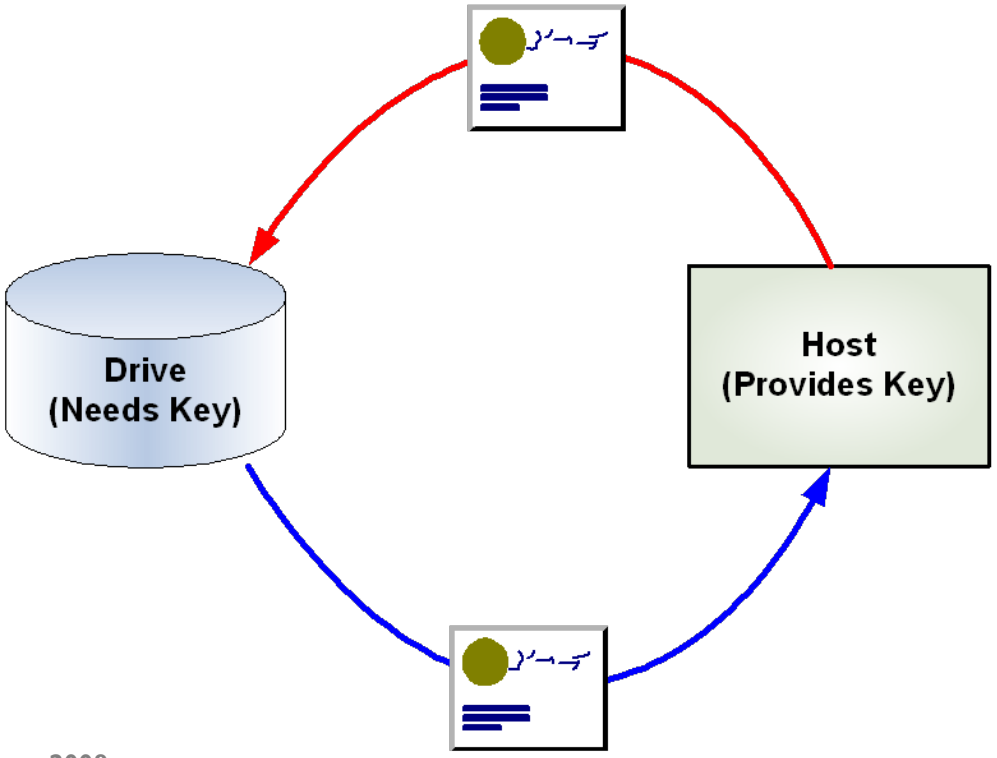
- Lock Key
- Authentication
- Drive Needs a Key for Any Access
  - Read Operations
  - Write Operations
  - Configuration



© 2008 Insert Copyright Information Here. All Rights Reserved.

Authentication

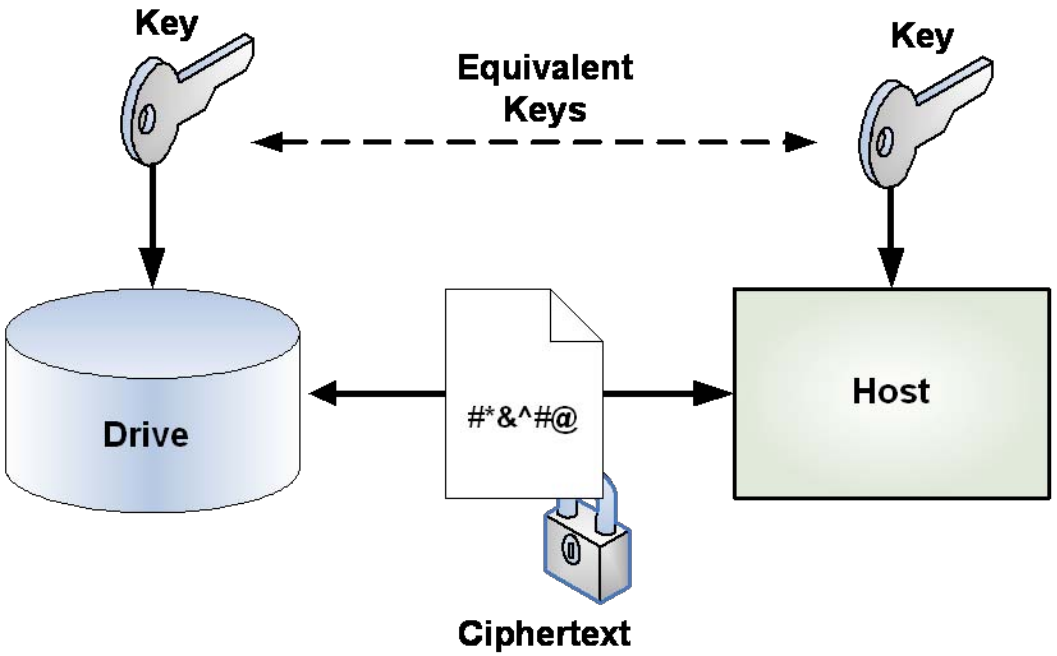
- Drive Authenticates Host
- Host Can Authenticate Drive



© 2008 Insert Copyright Information Here. All Rights Reserved.

Secure Messaging

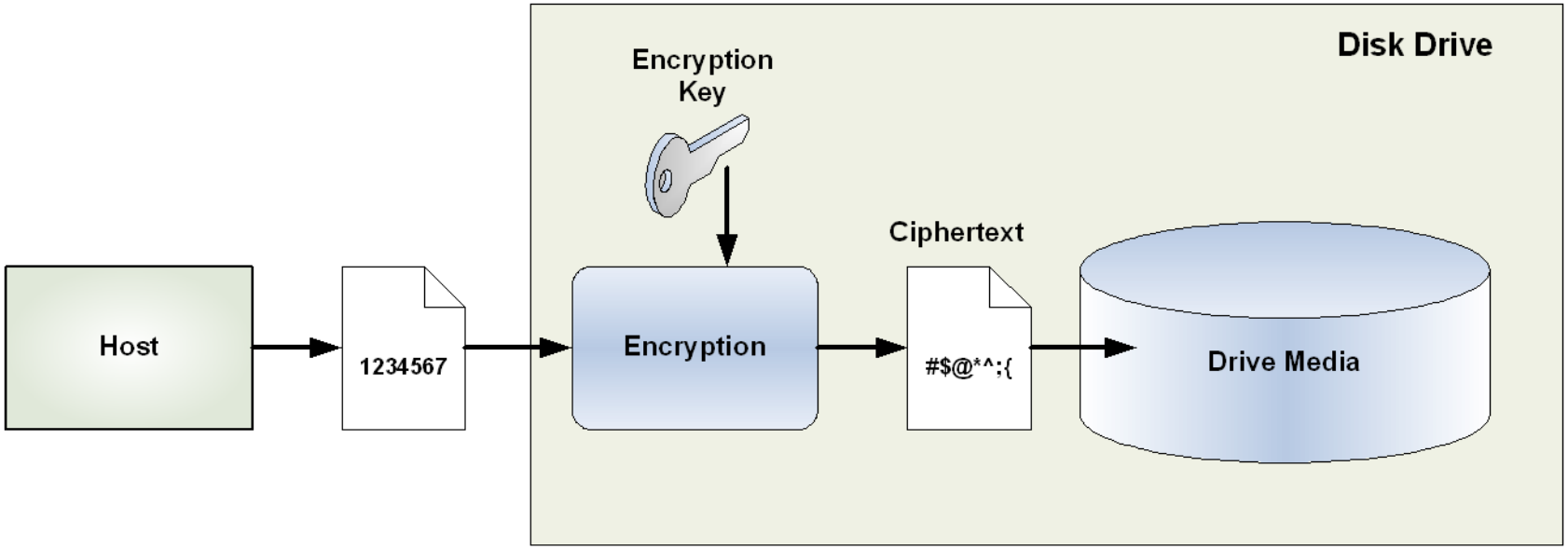
- Drives Agree on Encryption Key
- Commands and Data To/From Drive are Encrypted
- Data In Flight (DIF)



© 2008 Insert Copyright Information Here. All Rights Reserved.

Data Encryption Key

- Used to Encrypt/Decrypt Data on Media
- Data At Rest (DAR)



© 2008 Insert Copyright Information Here. All Rights Reserved.


KEYS! KEYS! KEYS!

Threats

© 2008 Insert Copyright Information Here. All Rights Reserved.

Disclosure

- Confidentiality
  - Key Disclosed to Unauthorized Entities
  - Data Accessible by Anyone
  - Authentication Failure
  - Eavesdropping
  - Improper Policies and Procedures

© 2008 Insert Copyright Information Here. All Rights Reserved.

Denial of Service

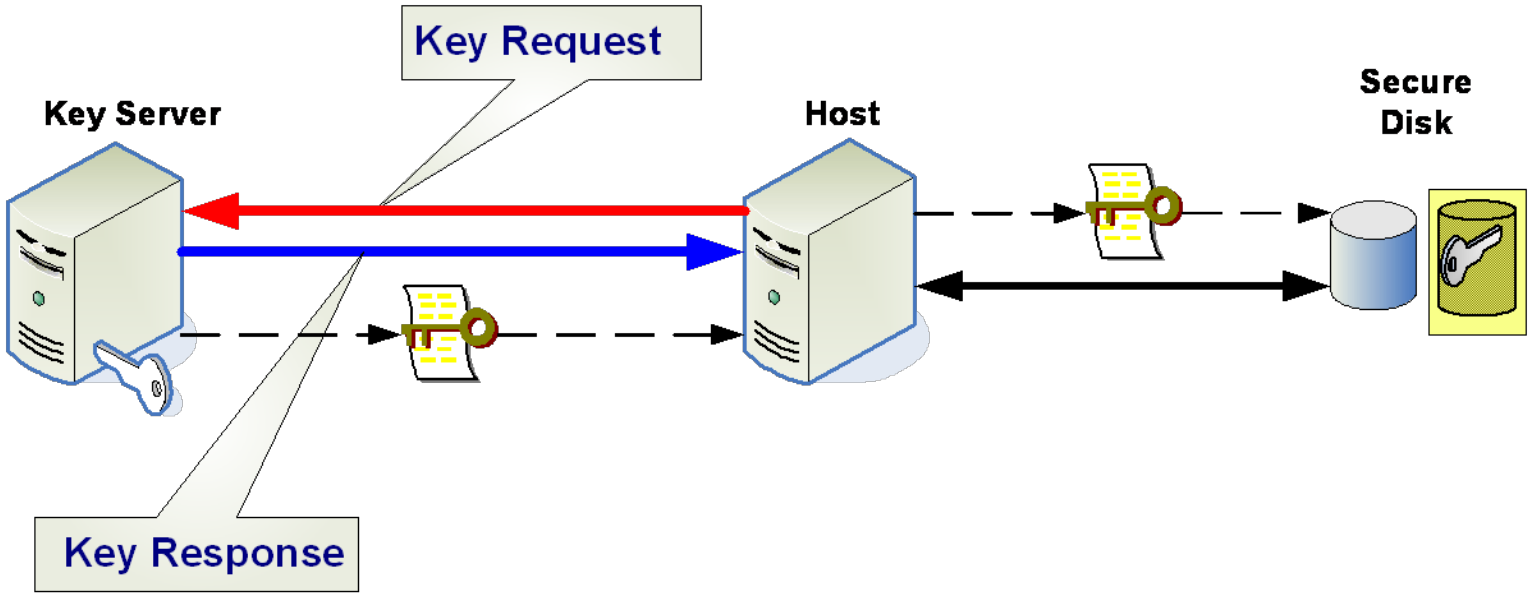
- Integrity
  - Key has Been Modified
  - Data Accessible by None
- Archive
  - Key has Been Lost
- Availability
  - Key Cannot be Accessed

© 2008 Insert Copyright Information Here. All Rights Reserved.

Key Management

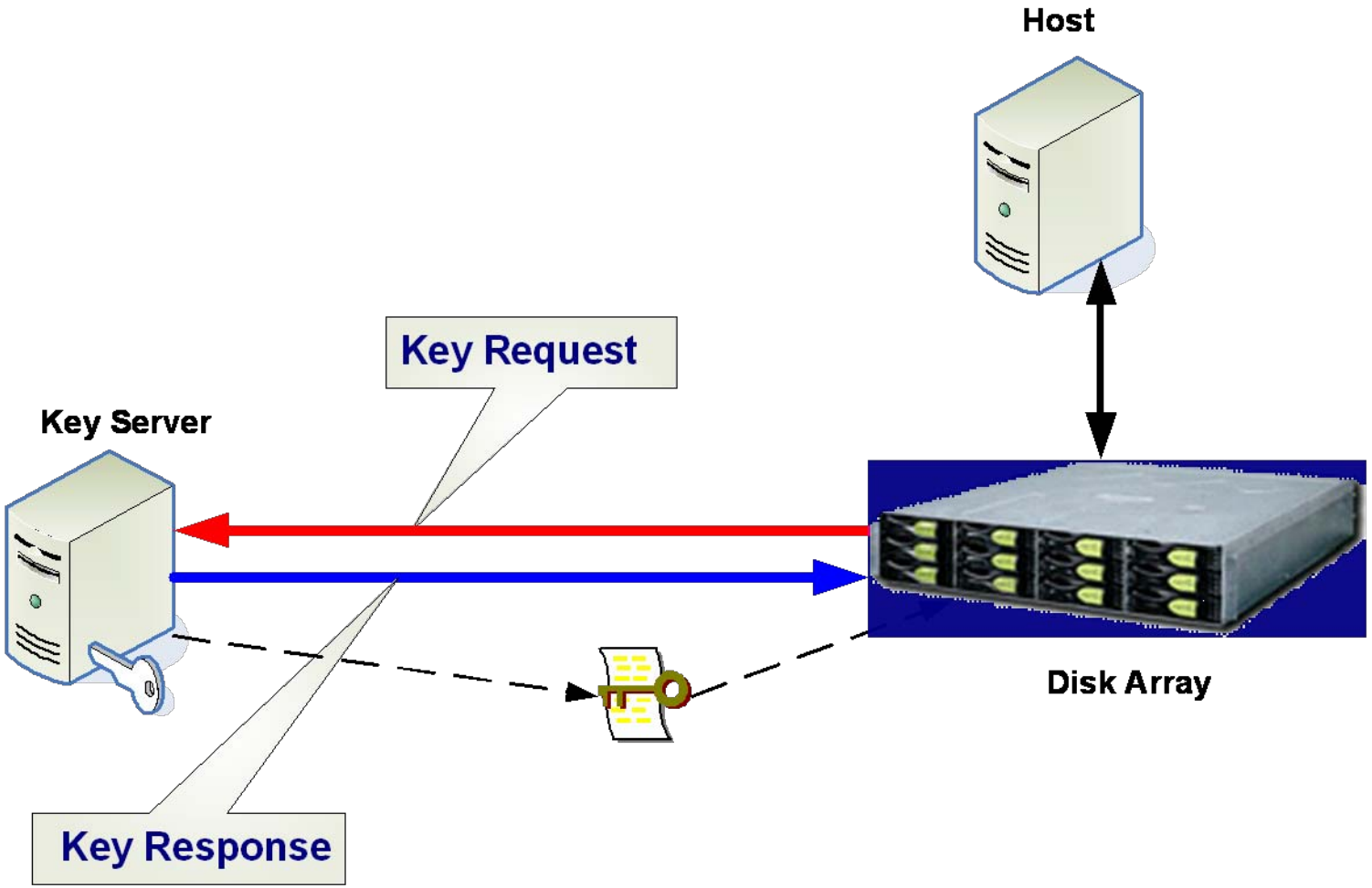
© 2008 Insert Copyright Information Here. All Rights Reserved.

Key Servers



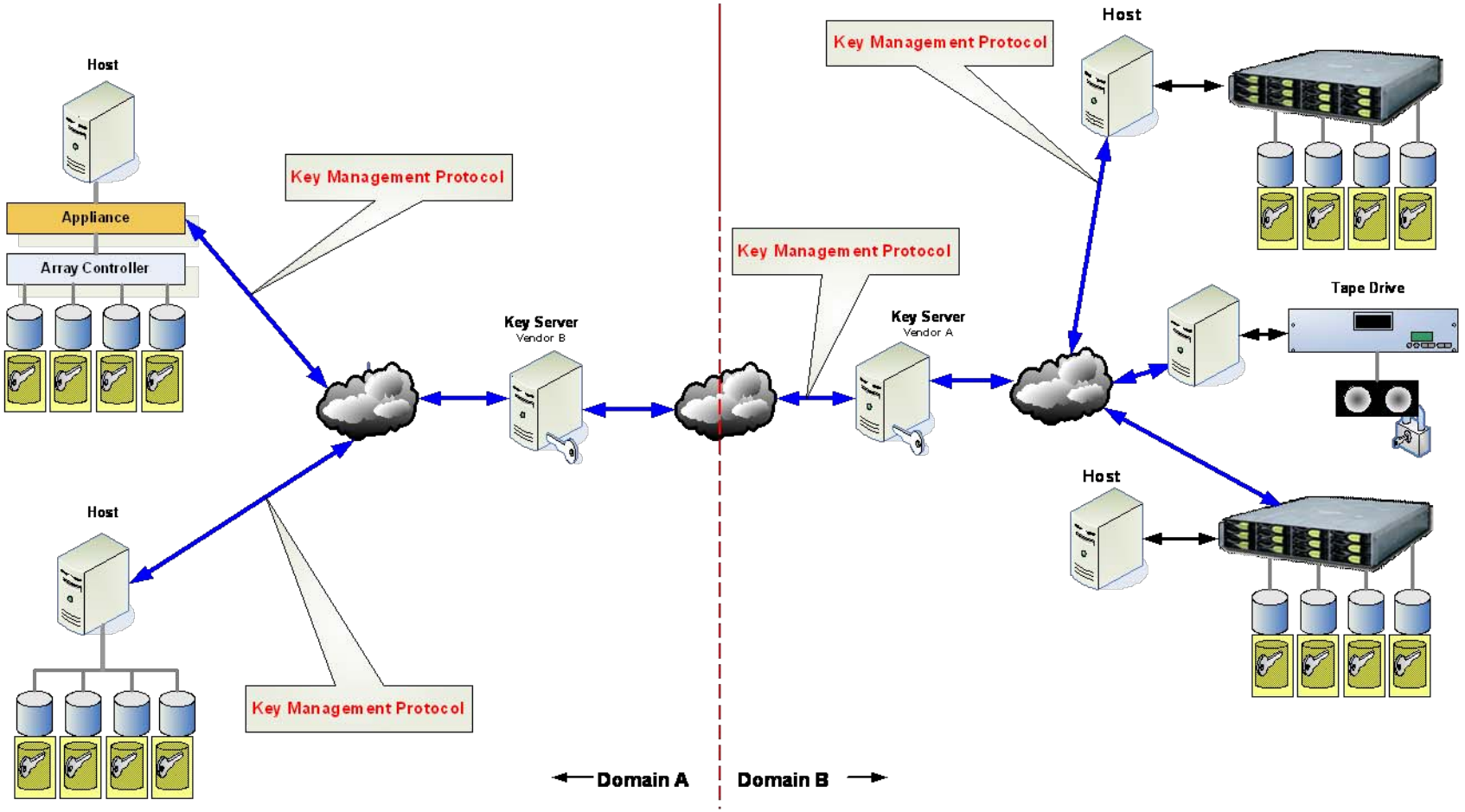
© 2008 Insert Copyright Information Here. All Rights Reserved.

Key Servers



© 2008 Insert Copyright Information Here. All Rights Reserved.

Key Management

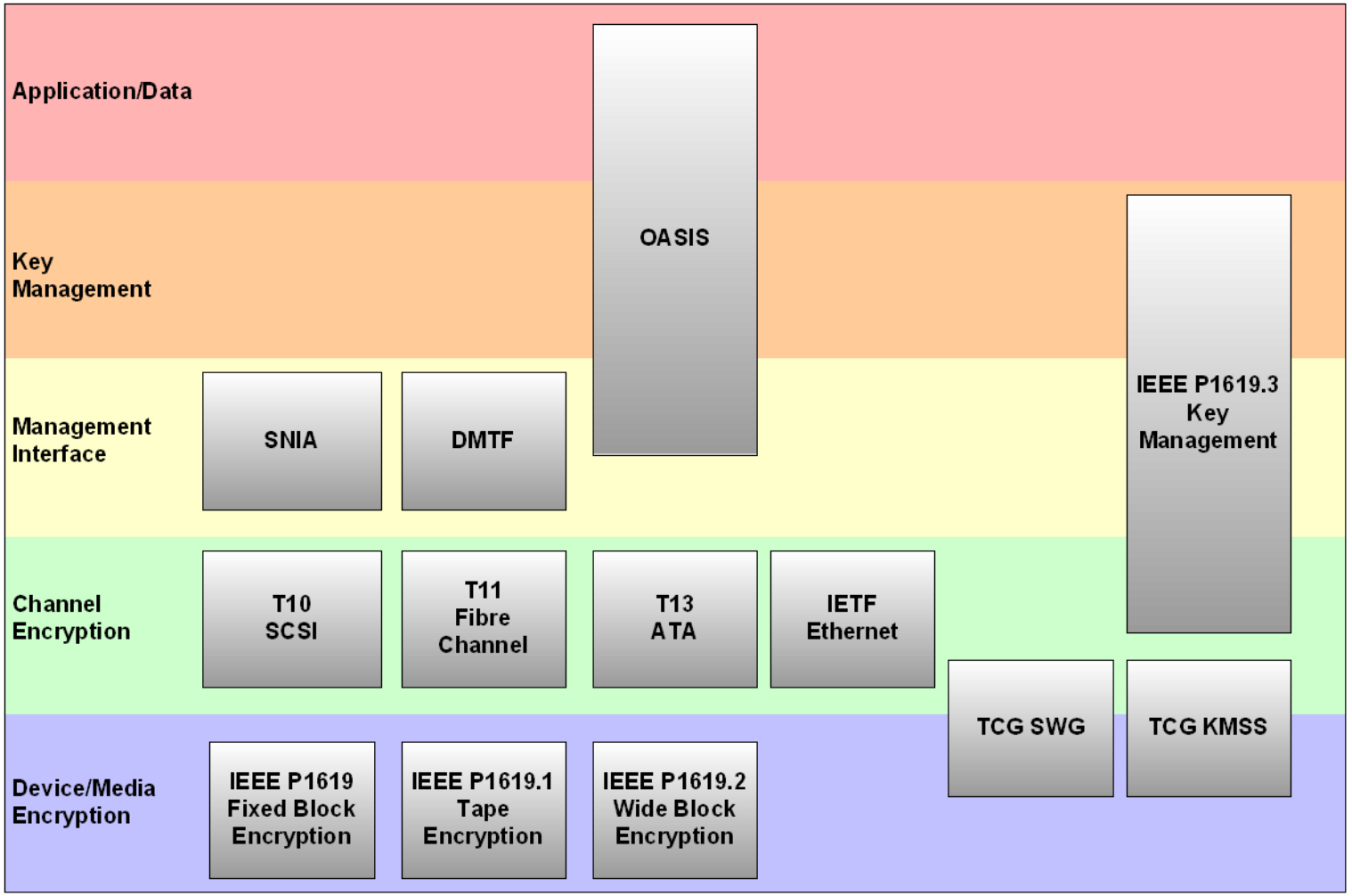


© 2008 Insert Copyright Information Here. All Rights Reserved.

Standards Organizations

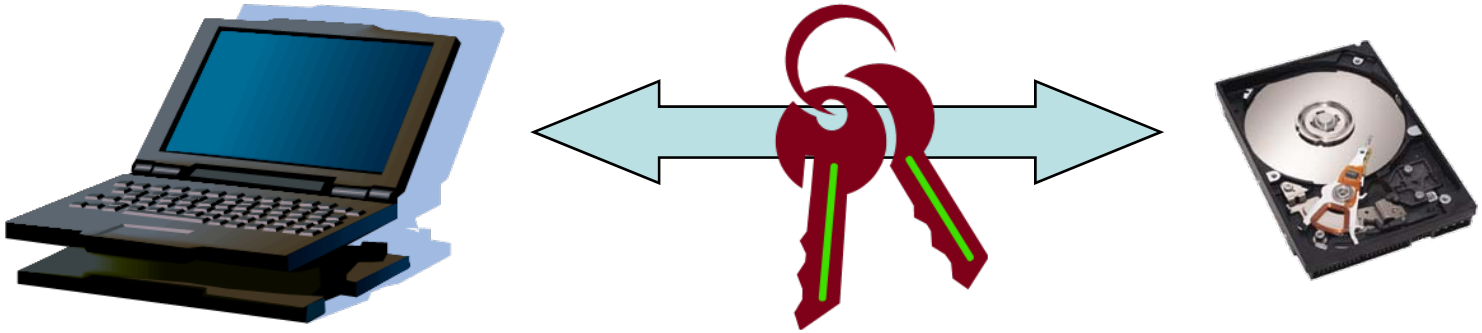
© 2008 Insert Copyright Information Here. All Rights Reserved.

Standards Groups



© 2008 Insert Copyright Information Here. All Rights Reserved.

TCG Key Management



- **Key Management Services Subgroup (KMSS)**
- **Define Best Practices for Key Management**
  - Mechanisms to Define and Manage Keys
- **Support for Any Device using the TCG Storage Specification**
  - A Uniform Way to Manage Keys for a Variety of Storage Devices
- **Application Support**
  - Ease Development with a Key Management Application Note

© 2008 Insert Copyright Information Here. All Rights Reserved.

TCG Key Management Operations

- **KMSS Addresses Operations Between**
  - **Host Platform**
  - **Application**
  - **Trusted Devices**

Host Platform

Application

Levels of Interaction and Security
Requesting Key Generation
Key Usage
Storage of Keys
Retrieving Keys
Modifying Keys
Searching for Keys
Key Access Rights
Disabling of Keys
Destruction of Keys

Trusted Device

© 2008 Insert Copyright Information Here. All Rights Reserved.

TCG KMSS Application Note

- Secure communication between the storage device and the host system.
- Authentication between the storage device and the host system.
- Discovery of the storage device capabilities.
- Compliance with existing data security regulations
- Flexibility to comply with future state and federal legislation.

https://www.trustedcomputinggroup.org/groups/storage/

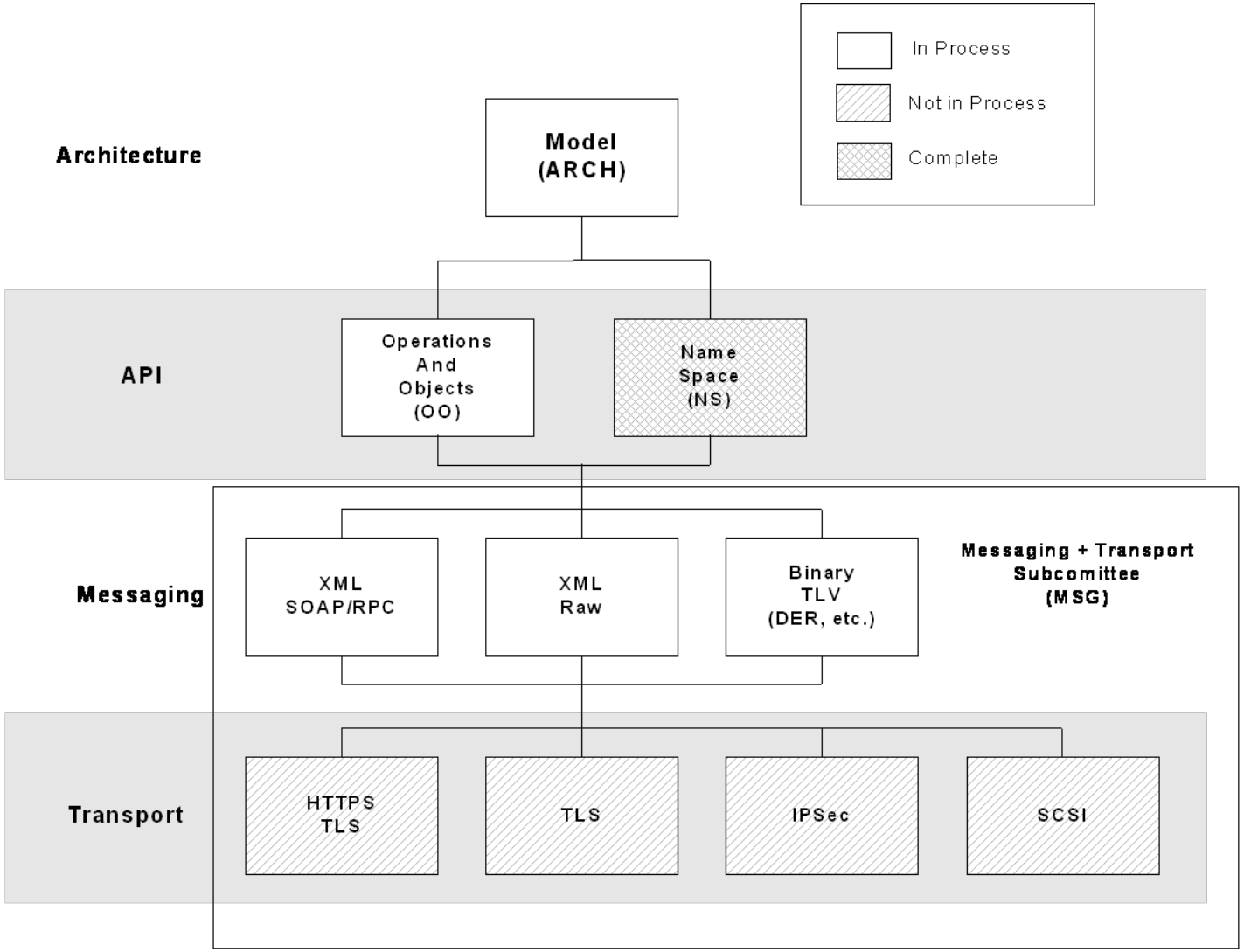
© 2008 Insert Copyright Information Here. All Rights Reserved.

TCG Future Application Notes

- Key Management for Tape Systems
- Key Management for Optical Storage
- Key Management for Consumer Devices
- Any Application of the TCG Storage Specification

© 2008 Insert Copyright Information Here. All Rights Reserved.

IEEE P1619.3



© 2008 Insert Copyright Information Here. All Rights Reserved.

Questions

© 2008 Insert Copyright Information Here. All Rights Reserved.

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
- FIPS 140-2: SECURITY REQUIREMENTS MODULES (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)
- Trusted Computing Group (https://www.trustedcomputinggroup.org/home)

© 2008 Insert Copyright Information Here. All Rights Reserved.

More Information

- 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)

© 2008 Insert Copyright Information Here. All Rights Reserved.