Education

Building a Key Management Strategy: Standards and Solutions

Robert A. (Bob) Lockhart
NeoScale Systems, Inc.

Abstract

Building a Key Management Strategy: Standards and Solutions

As storage security devices proliferate across highly heterogeneous user environments, key management standards are multiplying, as well. From PKI to P1619.3 to OASIS and the various others standards, it can be a challenge understanding what the standards represent and how they benefit your organization. This session, led by a recognized storage security expert, covers all of the key management standards that exist and where each fits in the scope of a comprehensive Key Management Services strategy.

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA.
- Member companies and individuals may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced without modification
  - The SNIA must be acknowledged as 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.

Storage Security Components

Authentication

Access Control

Integrity

Confidentiality

=

Basics of Information Assurance

- Storage security elements
  - Authentication – validates user, system and/or application
  - Access Control – determines what can be seen
  - Integrity – validates data is in the original state is was stored
  - Confidentiality – use of encryption to protect data content
- Encryption key management
  - If the key is lost or compromised, then so is the data
  - Keys must be available ***whenever*** and ***wherever*** data is accessed

Secure key management is the last challenge of storage security

Points of Data at Rest Encryption

Encryption at any point in the path

- Application
- Operating System
- File System
- Host Agent
- Hardware Accelerator
- Custom Encryption
- Appliance Encryption
- Switch Encryption
- Storage Controller
- Media Encryption

Who Should Be Involved

- Applications, server & storage management
  - Who owns the SLA for a service?
  - Who gets called when someone cannot access data?
- Information security management
  - Who owns information security?
  - Who makes security decisions?
- Compliance management
  - Who works with auditors?
  - Who monitors current and upcoming regulations?
- Auditors
  - Involve them up front to make sure it meets the requirements!!!
- Legal
  - Only if they have been involved before or if the regulation is very vague
  - This may open a can of worms but don't be afraid to ask questions

Staffing Coverage

- Staffing and training requirements
  - Who is responsible
  - Who maintains it all
  - Who do you trust
- Roles and responsibilities to consider
  - Administrators – configuration & deployment
  - Security – security & policy
  - Recovery – information recovery
  - Auditors – they keep us honest
  - Key Managers – control encryption keys

Secure Key Management Challenges

- Random key creation to ensure data privacy
- Key distribution for multi-site access
- Compliance requirements for long term archive
- Sharing encrypted data with business partners
- Recovery of encrypted data and keys at any site
- Data destruction across multiple locations

Education

Key Management Services

The Components of Key Management

Terminology

Term	Acronym	Definition
Key Management Service	KMS	The service as a whole and all functions there in.
Key Management Server	KM Server	Provides one or more services in a KMS system
Key Management Client	KM Client	Communicates with the KM Server or servers to access keys, policies and logs
Cryptographic Unit Agent	CU Agent	Provides a translation interface between a CU and the KM Client.
Cryptographic Unit	CU	Provides encryption of data or media
Key Management User	KM User	Human or automated user of KMS
Key Management Policy	KM Policy	Defines one or more requirements as it pertains to a key, including options for using keys

Key Management Service (KMS)

- Defines all aspects of key management that include but are not limited to:
  - Key generation
    - Cryptographically sound random bit and random number generation
  - Key storage
    - Secure key repository
  - Key lifecycle management
  - Policy management
  - Audit and accounting
  - Secure Time Stamping
  - User interface
- The service cloud consists of one or more servers performing one or more of the functions listed above
  - The service requires both client to server and server to server communications mechanism

Key Management Services Components

KM Server

Provides Secure Key Repository, Key Lifecycle Management, Policy Management, Audit/Reporting and Secure Communications for KM Clients and KM Users

Name Space, Objects, Message Format and Transport

KM Client

Communicates directly with KM Server using standard messaging and communications protocols such as XLM over TLS, XLM SOAP over HTTPS, or whatever we come up with. Communicates with CU Agent via Open API usually within the same system as CU Agent

KM Client API

CU Agent (Optional – usually built into CU or KM Client)

Provides translation from native CU protocols to KM Client API for storing and requesting keys, policies and other cryptographic information required to encrypt data at rest. Will usually reside on same system as KM Client.

Application Specific Communications

Cryptographic Unit (CU)

Provides encryption of data either at rest or in flight. Uses message formats and protocols defined by appropriate standards bodies to communicate with a controlling entity (array, library, host OS, etc…

NOTE: If it is in **Red** or in a Red box, it must be defined by a KMS standards group

Key Management Server (KM Server)

- KMS server that provides specific functions that may include one or more of the following:
  - Key lifecycle management
  - Policy management
  - Audit, accounting and reporting functions
  - Secure key repository
  - KM User console
- Server should provide lookup functions for associated clients
  - Similar to DNS Client, talks to one or more servers that in turn can find keys that are not kept locally

Key Management Client (KM Client)

- Provides communications directly between Cryptographic Unit/CU Agent and KM Server
  - Cryptographic unit and KM Client can exist in a single
- At a minimum KM Client must authenticate to one KM Server
  - Mutual Authentication is recommended
  - Use of certificate based authentication recommended
    - Should not force the requirement of a full PKI implementation
- Transactions and sessions should be based on existing standards

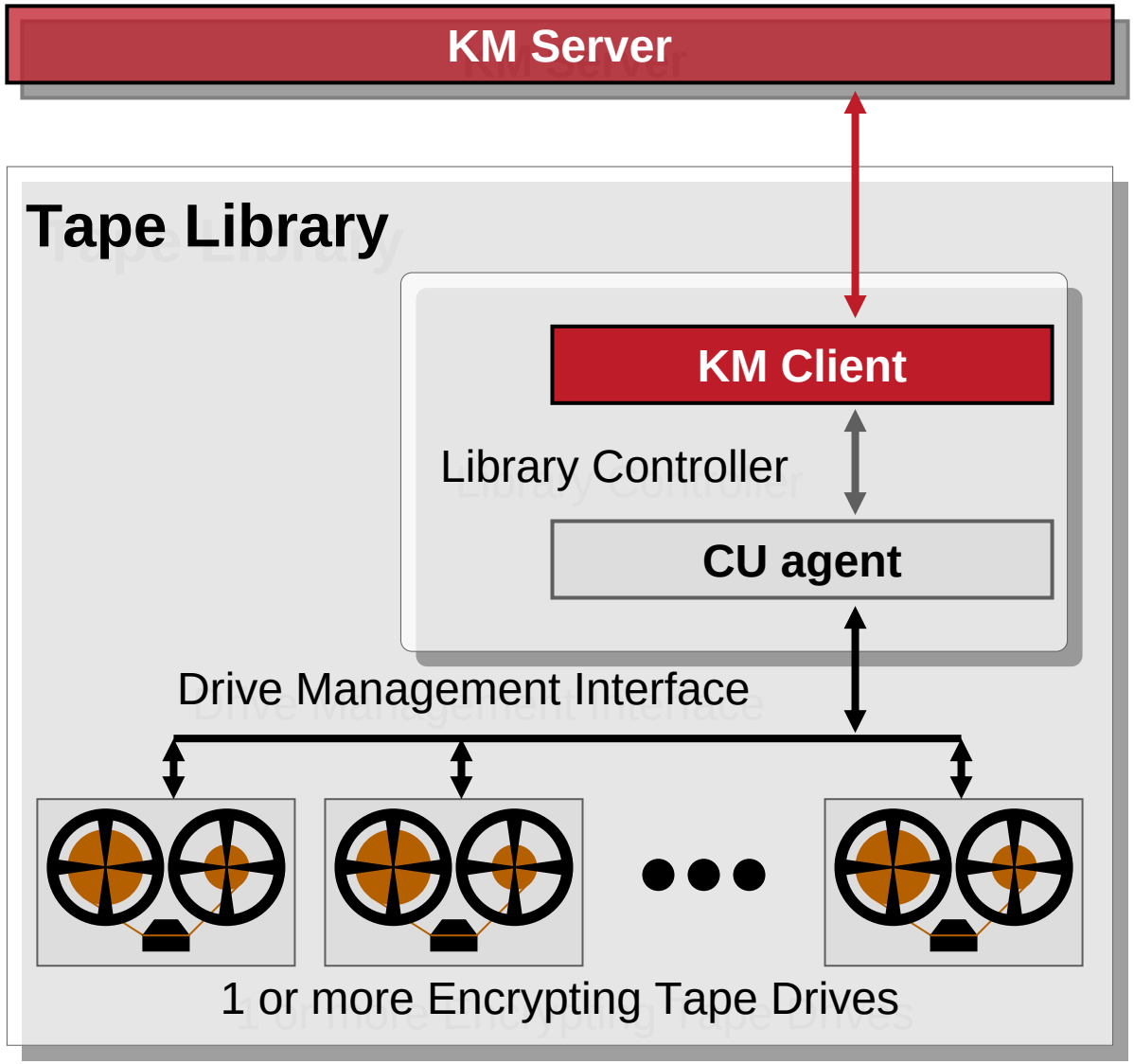
CU Agent (Optional)

- Provides a proxy interface between KM Client and Cryptographic Unit
  - Translates CU requests into KMS API calls
  - May or may not be integrated with the KM Client to form single entity
- Existing devices will probably require the use of a CU Agent
  - Devices that perform encryption but don't have a standard interface would use a CU Agent to communicate with KM Client
  - Most encrypting devices available today fall into this catagory and would require an external CU Agent and KM Client or consolidated CU Agent/KM Client to communicate with the KM Server
- Cryptographic Units that have KM Client built in will usually not require the CU agent

Cryptographic Unit (CU)

- User of keys to encrypt and/or decrypt data. Unit where cryptographic functions takes place.
  - May or may not contain the KM Client
- Existing devices will usually fall into this category
  - Devices that perform encryption but don't have a standard interface would use a CU Agent as a proxy to communicate with KM Client via Open API
    - This can include existing vendor specific key management applications or devices
  - LTO4 falls into this device and would require an external KM Client

Sample Application – Tape Library



Education

Key Management Services

Mapping Business Policy and Key Management Policy

Business Policy

- A policy that is high level in description and dictates what is to be done
  - e.g. IT will protect customer data with considerations for regulatory compliance, business requirements and appropriate level of risk associated with the type, classification and volume of data being protected
  - Any protection mechanism usually means more than one method for providing security
  - Encryption is an acceptable form of protection for most regulatory compliance when used with other forms of protection
- Encryption is usually the last line of defense

Mapping to Security Policies

- Security Policy defines how data is to be protected
  - Hopefully, based on some form of data classification
  - Security should have an understanding all the options available for protecting the data
    - While it may sound good no one solution meets all security requirements
- Security is handed a business policy and must derive a security policy from it
  - This is usually aided by utilizing existing tools such as ISO 17799 (BS7799) or other such standards
  - Encryption is one of the tools that security may define as a data protection mechanism to meet regulations that are a “little vague”
- Security and/or auditors will usually include auditing and reporting requirements in a security policy
- Security may have metrics and measurements that must be kept to test security of the data
  - Regularly scheduled testing may be required in some cases

Key Management Policy (KM Policy)

- Define automatic controls as they relate to keys that include but are not limited to:
  - Key generation requirements
  - Key length and strength
  - Retention and re-keying requirements
  - Distribution and replication
  - Usage (i.e. encrypt only / decrypt only / both)
  - Auditing requirements
  - Key granularity
  - Access control
  - Key storage requirements

Key Management Policy as part of Business Policy

- Key Management policies are the basic building blocks for ensuring that encryption meets a specific set of requirements that are defined by a Security Policy which was defined to meet a specific Business Policy
- Multiple KM Policies may be required to meet the specific Business Policy requirements
  - Key strength, access control, retention policy, key granularity and audit requirements are required to meet certain requirements in the PCI DSS
    - PCI DSS – Payment Card Industry Data Security Standard
- Auditors, Information Security, Storage and Systems Administration should all be involved in ensuring policies are being met and enforced properly
  - Occasionally Lawyers may be required as well… egad.

SNIA

Education

Key Management Services

Regulatory Requirements and Key Management

Some Regulations Require Data Protection

- Global Regulations
  - USA – Sarbanes Oxley
  - USA – Graham, Leach, Bliley Act (GLBA)
  - USA & Canada – Health Insurance Portability and Accounting Act (HIPAA)
  - State privacy laws
    - California SB1386, AB1950 & several more pending…
    - New York State Information Security Breach And Notification Act
  - EU – Data Privacy Directive
  - Japan – Personal Information Protection Act
  - A whole bunch more where these came from…
- Companies need to plan for all regulations and if encryption is used proper key management and logging are required

Regulatory Requirements

- All regulations that specify data protection may or may not require or recommend encryption
  - Very few regulations say the words encrypt or encryption, but in some cases it is the only way to meet the intent of the law
- Those that do, require proof that encryption has occurred
  - Proof from logging is not always the only accepted method
  - Varies from auditor to auditor
- If media is replaced, destroyed or lost keys will have to be destroyed or re-keyed to ensure the data is gone
  - A complete audit trail from creation to destruction of a key will most likely be required
- One layer of encryption may not meet regulatory requirements in the long run!
  - By encrypting at the application and at the media level it may be possible avoid certain re-keying requirements such as replaced media, application migration, etc…

Education

Key Management Services

Staying one Step Ahead…

…of the Law

Protecting the Keys

- Never send a key in the clear
  - ON ANY TRANSPORT
  - There are inline analyzers for every media
- Use split knowledge when exporting keys
  - This requires two or more persons or media to come together to reform the key
  - May be referred to a K of N, M of N or Quorum
- Securely storing the keys
  - On the media with the data
    - Can be done but understand the consequences
    - Lose the media, how was the key protected?
  - Secure repository
    - Best bet
    - Provides secure access to keys only when needed
    - Should have no concept of how a key is protected (wrapped/encrypted) when performed by software

Re-keying of Data is Required

- Most regulatory compliance does not require re-keying…
  - However it is recommended as a best practice for Data at Rest to re-key at least once every 12 months…
    - What about that tape in cold storage for seven years?
    - What about that encrypted CD I lost?
  - PCI DSS requires re-keying of data every 12 months
    - This is based on human accessibility to keying material and the potential of exposure as well as time, key usage
    - The jury is still out on re-keying offline stored (tape) data although it has to be encrypted

Why Re-key?

- Re-keying based on a set time may not meet the letter of the law if…
  - You encrypt more data than the key was meant to…
    - AES amount of data varies from mode to mode with new IEEE P1619, P1619.1 and P1619.2 modes starting at 2^{64}-1 bytes (16 exobytes) before hitting the birthday bounds
  - The possibility exists that the key was exposed
    - If the possibility exists you should consider it as having happened…
    - Better safe than sorry!
  - Elvis has left the building
    - Someone with control of the keys has departed the organization or changed job functions

Logging is NOT an Option

- Securely log events for a key – throughout its lifecycle
  - When a key is created, distributed, used, stored, disabled, re-enabled, exported, used again and finally destroyed
    - Each should have the person, persons or device performing the act
  - Cryptographically signing an individual log entry while optional is highly recommended
  - Calling it what it is: CYA (cover your assets)
- Understand the difference between secure audit logs and traditional event logs
  - Audit logs will be signed and protected from modification, deletion or tampering
  - Event logs are SNMP, remote system logging, email alerts, etc… with security as an option but usually not implemented

Education

Key Management Services

Key Management Standards

Public Key Infrastructure (PKI)

- A method of using Public and Private Keys
  - Performs both authentication and encryption depending on how certificate is used
  - Public keys are for anyone to see and use
  - Private keys are held by the owner of the keys
- Public Keys are authenticated using Certificate Authorities
- For encryption public keys are used to encrypt and private keys are used to decrypt
- Used for authentication in web servers (HTTPS)
  - CA authenticates certificates to client
  - It is possible to use self signed certificates but that can lead to other isses
- Common Uses of PKI include:
  - Encrypting email
  - Signing documents
  - Authentication

Public Key Cryptography Standard (PKCS)

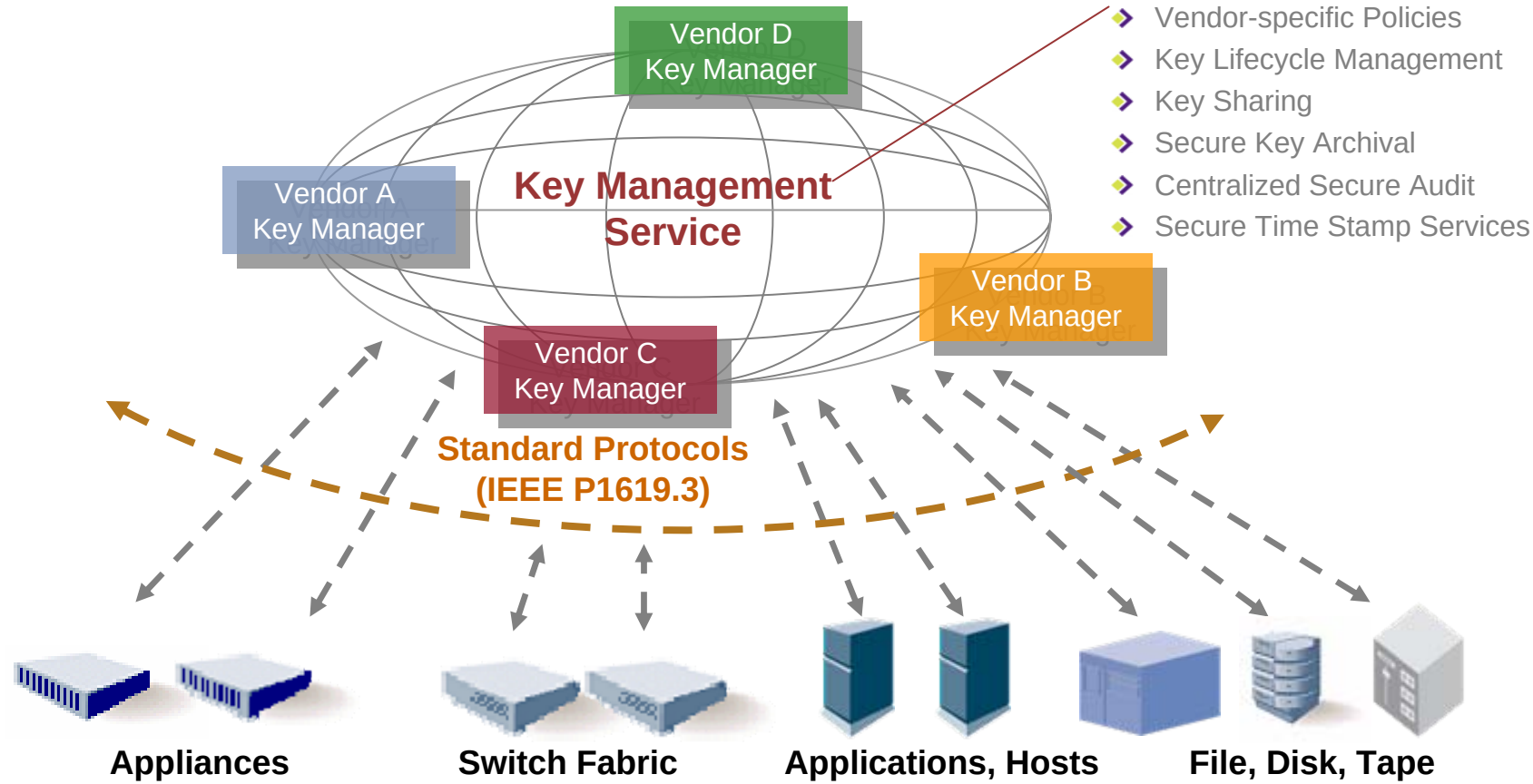
- Developed by RSA
  - Provided to promote the use of PKI
  - Not formally a public standard but there is work being done here by groups such as IETF PKIX workgroup
- Helps define standard methods of using Public Key Infrastructure for encryption and authentication
  - Helps to ease the use of Public Key technologies by creating a set of public “standards”
- Currently 15 different PKCS standards are defined or being defined
  - PKCS#2 and PKCS#4 have been merged into PKCS#1
  - PKCS#13 and PKCS#14 are still in development
- Existing versions modified by RSA Labs as needed or required
  - PKCS#1 is currently at version 2.1
  - PKCS#11 is currently at version 2.2

IEEE Key Management Service Network:
P1619.3 Standard (in development)

Education SNIA

Standard API sets and Protocols for Multi-Vendor Key Management and Encryption End Point Communication

- Key Policy Administration
- Vendor-specific Policies
- Key Lifecycle Management
- Key Sharing
- Secure Key Archival
- Centralized Secure Audit
- Secure Time Stamp Services



Supporting a Range of Local Key Services on Encryption End Points

IETF KEYPROV (in development)
CT-KIP and Dynamic Symmetric Key Provisioning Protocol

- A protocol specification that combines:
  - All Cryptographic Token-Key Initialization Protocol (CT-KIP)
  - Dynamic Symmetric Key Provisioning Protocol (DSKPP) features not explicitly addressed by CT-KIP
- A key container specification based on the Portable Symmetric Key Container
- CT-KIP
  - A client-server protocol for initialization and configuration of cryptographic tokens with shared keys
  - Intended for general use within computer and communications systems employing connected cryptographic tokens
- DSKPP
  - A client-server protocol that enables a client device to download and install authentication credentials from a provisioning server
  - The protocol is for dynamic provisioning of shared secret to a user device

OASIS (in development)
Enterprise Key Management Infrastructure (EKMI)

- **A collection of technology, policies and procedures for managing all cryptographic keys - symmetric and asymmetric - in the enterprise**
  - It allows enterprises to define cryptographic key-management policy in a single place
  - It provides secure protocols for availing key-management services from servers configured for this purpose
  - It is platform and application-independent
  - It is scalable to accommodate the needs of an enterprise of any size
  - It is redundant to provide cryptographic services even in the face of network failures
  - It is extremely secure

Conclusion

- Encryption key management is not just about storing keys
  - Key storage, lifecycle, policy, logging and reporting are all part of a complete KMS
- Additional thought should be given to any solution whose keys are going to exist for more than a few hours
  - Determine what your organizations requirements are before implementing any solution
- Policies on managing and maintaining keys should be created prior to implementation
  - Modify as needed based on lessons learned!
- Secure logging is a mandatory requirement of any Key Management Service
  - Make sure the logging meets corporate and regulatory requirements
- Ensure the selected solution has the ability to meet forthcoming standards

Q&A / Feedback

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

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

SNIA Education Committee

Matt Ball, Quantum
Larry Hofer, Emulex
Landon Curt Noll, NeoScale
Eric Hibbard, HDS
Walt Hubis, LSI Logic