Key Management and the Storage Eco-system

Tim Hudson
CTO @ Cryptsoft
tjh@cryptsoft.com

Abstract

- Security and Storage covers a diverse range of technologies and approaches that can make it challenging to distill a workable strategy from the mix of architectures, tools, techniques, recommendations, standards and competing vendor solutions. Guidance on how to contrast the various security approaches in storage and evaluate the right mix for your specific problem domain forms the majority of the material covered in this session.

Key Management and Storage

PROBLEM ORIGIN

Why add Security?

- Regulatory obligations
- Legal requirements
- Corporate requirements for confidentiality
- IS/IT requirements

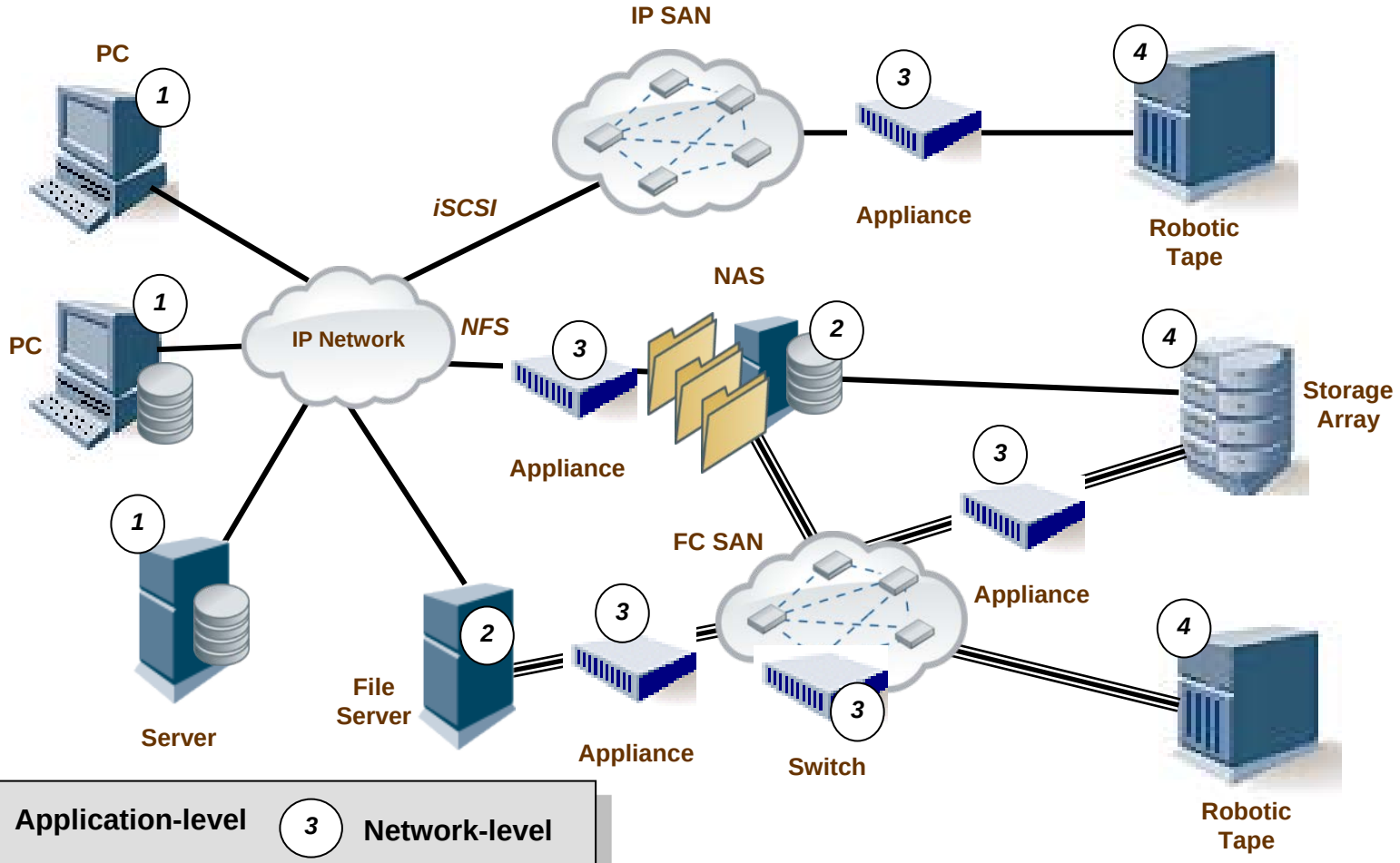
Benefits of Data Encryption

- Confidentiality
- Integrity
- Control
- Peace of Mind

Key Management and Storage

ECOSYSTEM - THEORY

Points of Encryption



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

General Points of Encryption

- **Application-level** – under control of application or database
- **Filesystem-level** – under control of the OS or OS-level app
  - e.g., NAS
- **Network-level** – under control of the network devices
  - e.g., HBA, array controller, or switch
- **Device-level** – under control of the end-device
  - e.g., Storage array, tape drives, etc.

Factors Influencing Encryption

Impact	Application	Filesystem	Network	Device
Usability	Low	Low-Moderate	None	None
Availability	Can be significant	Can be significant	Low-Moderate (Redundancy)	Low-Moderate
Infrastructure	Can be significant	Can be significant	Low-Moderate	Low
Performance/ Throughput	Can be severe	Can be significant	Low	Low-Moderate
Scalability	Can be significant	Can be significant	Can be moderate	Minimal
In Motion Confidentiality	Excellent	Low-Moderate (NAS); Excellent (Host)	Low-Moderate	None
Business Continuity / Disaster Recovery	Can be extremely complicated	Can be complicated	Can be extremely complicated	Can be extremely complicated
Proof of Encryption	Can be complicated	Relatively easy	Low-Moderate	Can be complicated
Environmentals	Low-Moderate	Low-Moderate	Can be significant	Low

Key Management and the Storage Eco-system

Key Management and Storage

THEORY to PRACTICE

Multi-Vendor – Who and Where

DATA STORAGE SECURITY SUMMIT

Storage

- Disk Arrays, Flash Storage Arrays, NAS Appliances
- Tape Libraries, Virtual Tape Libraries
- Encrypting Switches
- Storage Key Managers
- Storage Controllers
- Storage Operating Systems

Infrastructure

- Key Managers
- Hardware security modules
- Encryption Gateways
- Virtualization Managers
- Virtual Storage Controllers
- Network Computing Appliances

Cloud

- Key Managers
- Compliance Platforms
- Information Managers
- Enterprise Gateways and Security
- Enterprise Authentication
- Endpoint Security

Multi-Vendor – What

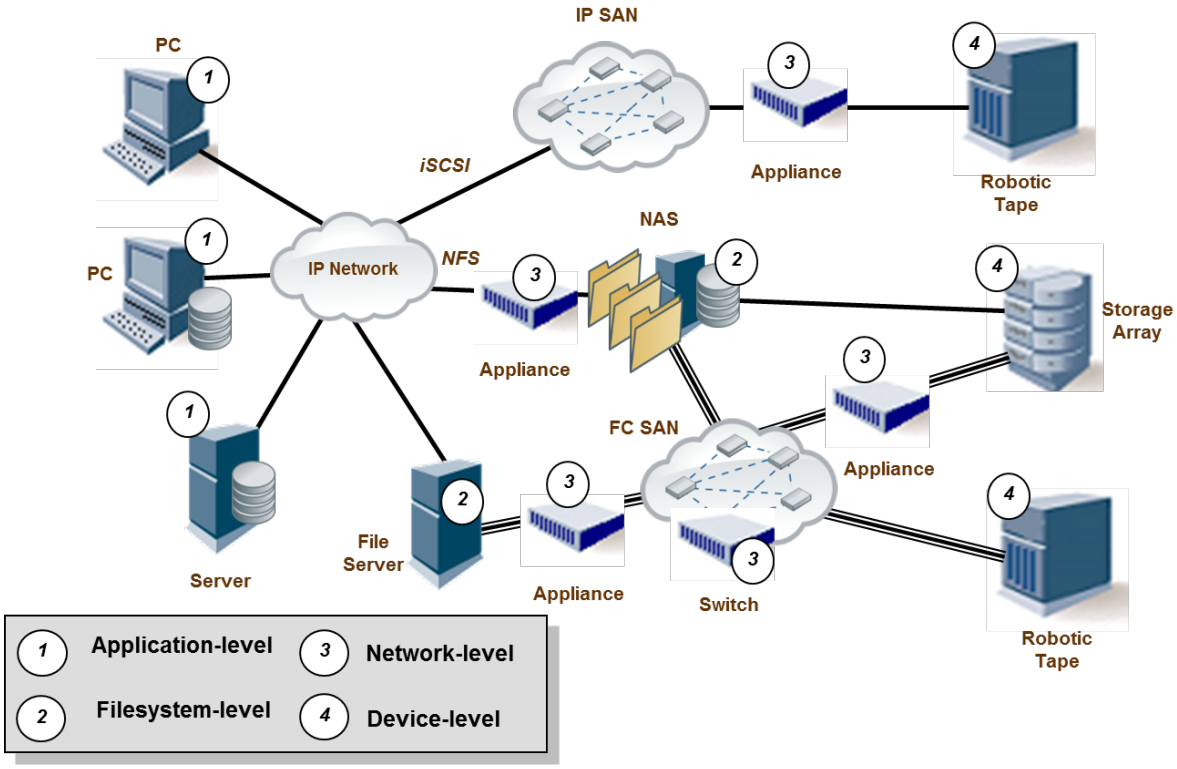
- Disk Arrays, Flash Storage Arrays, NAS Appliances, Storage Operating Systems
  - Vaulting master authentication key
  - Cluster-wide sharing of configuration settings
  - Specific Usage Limits checking (policy)
  - FIPS140-2 external key generation (create, retrieve)
  - Multi-version key support during Rekey
  - Backup and recovery of device specific key sets

Multi-Vendor – What

- Tape Libraries, Virtual Tape Libraries
  - External key generation (create, retrieve)
  - FIPS140-2 external key generation (create, retrieve)
  - Multi-version key support during Rekey
- Encrypting Switches, Storage Controllers
  - Vaulting device or port specific encryption keys
  - Cluster-wide sharing of configuration settings
  - Specific Usage Limits checking (policy)

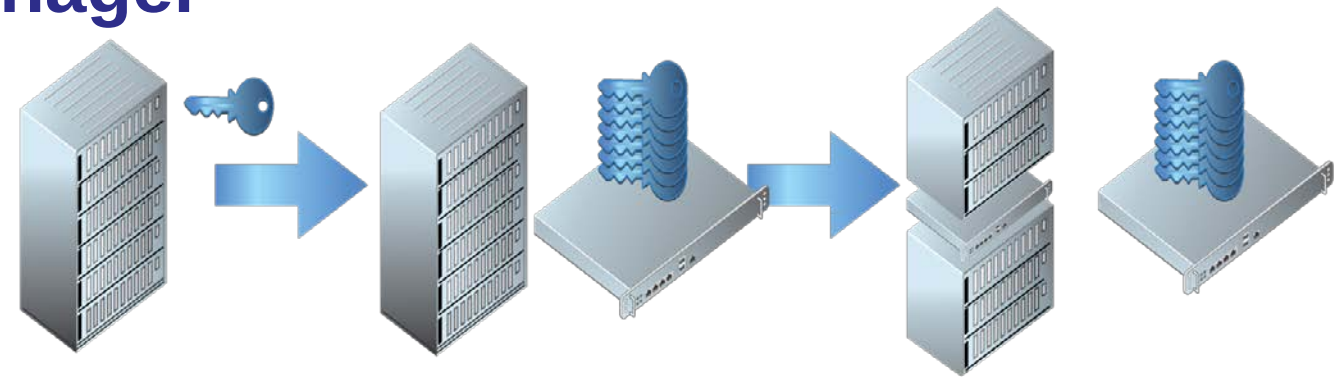
KMIP – Adoption (Storage)

- **KMIP is present in the following:**
  - Device-level
    - Disk arrays
    - Tape libraries
    - Virtual tape libraries
    - Flash storage arrays
    - Storage controllers
    - Storage operating systems
  - Network-level
    - Encrypting switches
  - File/Object-level
    - NAS appliances
  - Storage key managers



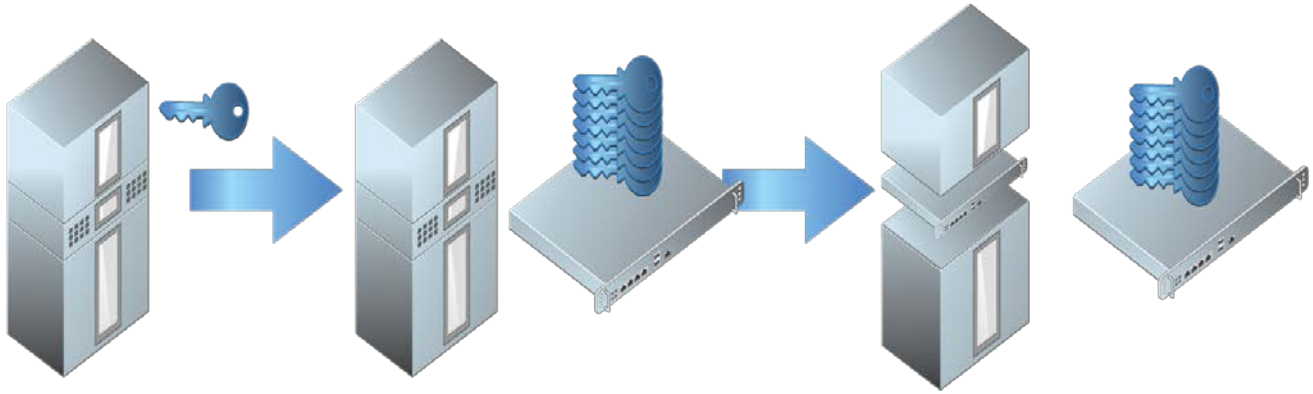
Disk Array Deployments

- **Traditional – array + connected key manager**
  - Identifiers or other unique reference stored locally
  - Common operations (Create, Register, Locate, Get, Destroy)
- **Emerging – array with embedded (proxy) key manager**



Tape Library Deployments

- **Traditional – Library + connected key manager**
  - Identifiers or other unique reference stored locally (on-tape)
- **Emerging – Library with embedded (proxy) key manager**



Key Management and the Storage Eco-system

Key Management and Storage

WHY IS IT IMPORTANT

Why is Key Management Important?

- Disclosure of key is disclosure of data
- Loss of key is loss of data
- Key availability is data availability

Why is Key Management Important?

- Is there one magic solution?
- Can I just avoid the whole issue?
- As a vendor – can I make this a problem for someone else to solve?
- As a customer – can I get some choice in how this is solved?

Key Management and the Storage Eco-system

Key Management and Storage

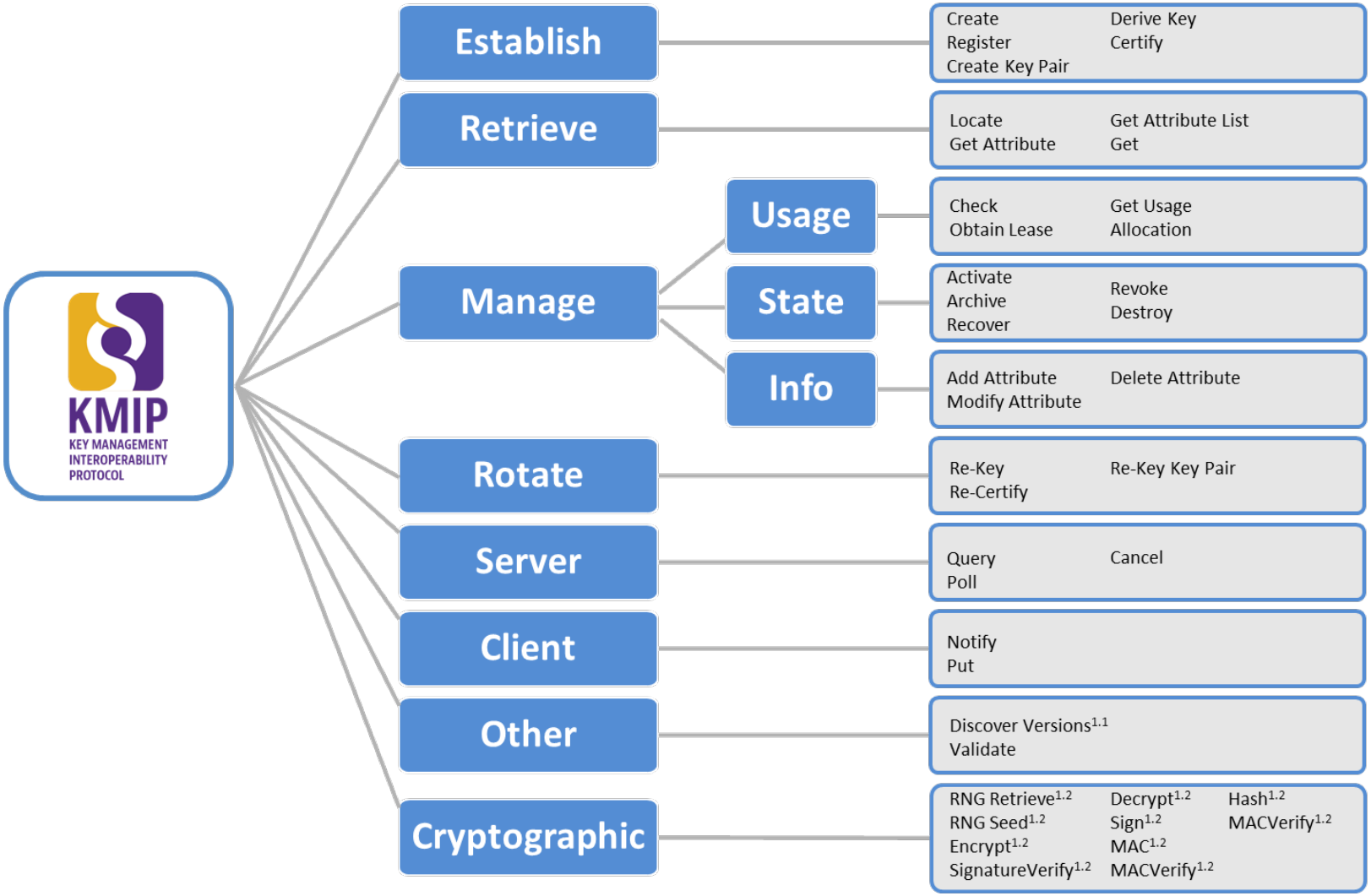
OASIS Key Management Interoperability Protocol (KMIP)

What is KMIP?

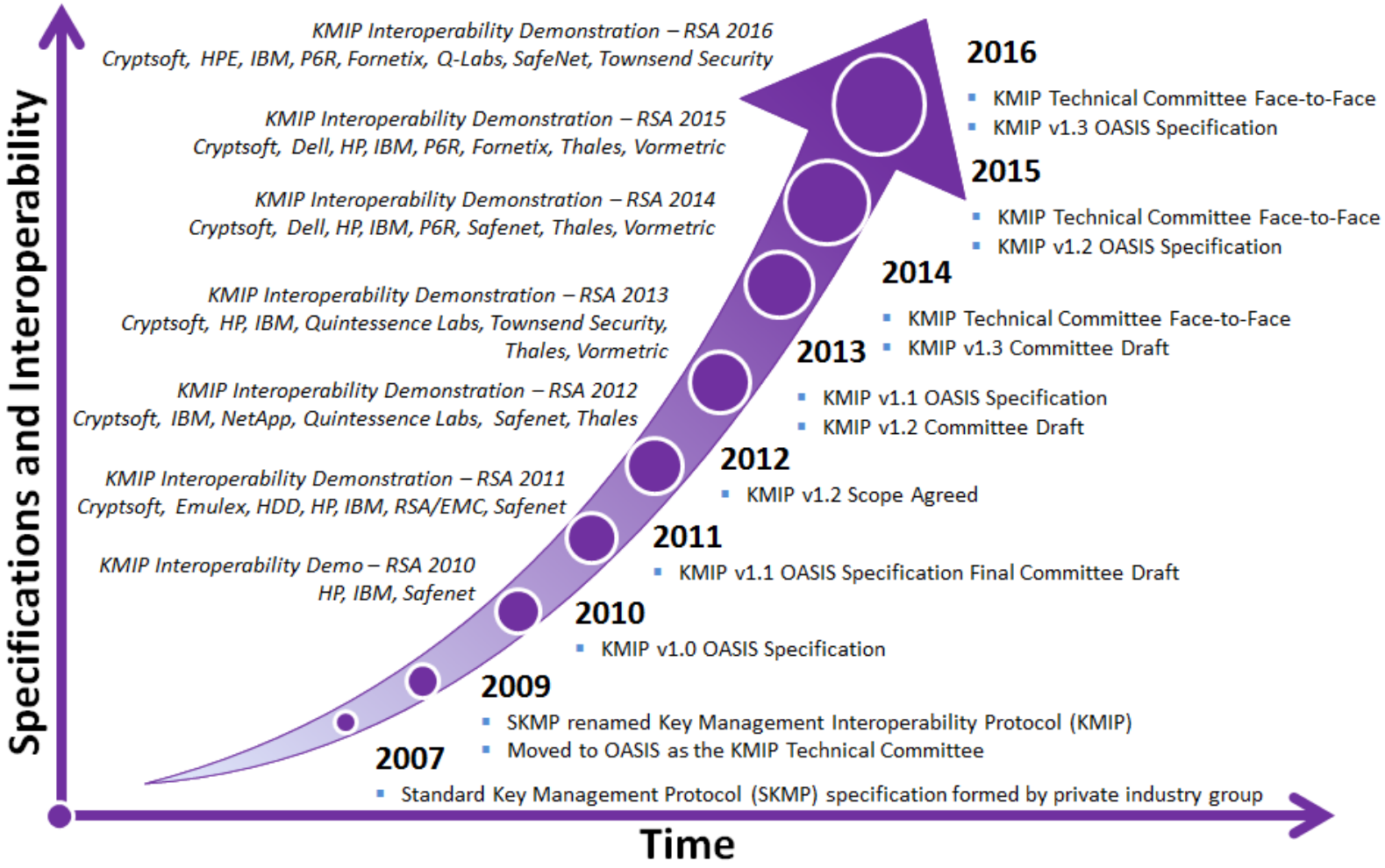
- Key Management Interoperability Protocol
  - “The OASIS KMIP TC works to define a single, comprehensive protocol for communication between encryption systems and a broad range of new and legacy enterprise applications, including email, databases, and storage devices. By removing redundant, incompatible key management processes, KMIP will provide better data security while at the same time reducing expenditures on multiple products.” - https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip
  - A protocol for enterprise management of “stuff”

- OASIS KMIP TC Membership (foundational and sponsor)
  - Cryptsoft, Dell, EMC, Fornetix, Futurex, Hancom Secure, Hewlett Packard Enterprise, IBM, NetApp, Oracle, SafeNet, Symantec, VMware, Vormetric

KMIP Fundamentals



KMIP Specification History



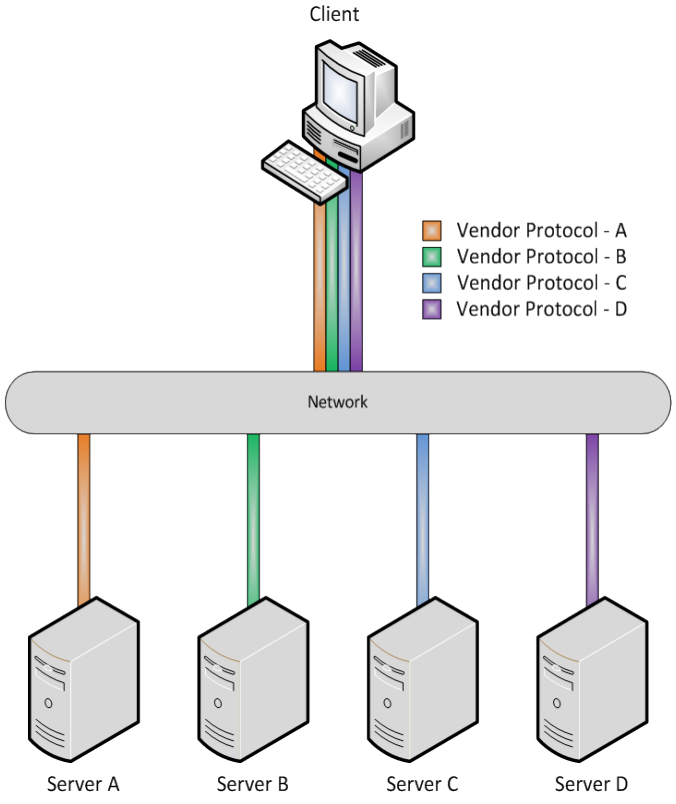
OASIS KMIP Specification

- OASIS KMIP 1.0 – PR Nov 2009, CS Jun 2010, OS Oct 2010
  - Specification 105 pages
  - Profiles 16 pages
  - Usage Guide 44 pages
  - Use Cases (Test Cases) 168 pages
- OASIS KMIP 1.1 – PR Jan 2012, CS Jul 2012, OS Jan 2013
  - Specification 164 pages +56%
  - Profiles 39 pages +143%
  - Usage Guide 63 pages +43%
  - Test Cases 513 pages +205%
- OASIS KMIP 1.2 – PR Jan 2014, CS Nov 2014, OS May 2015
  - Specification 188 pages +14%
  - Profiles (multiple) 871 pages +2133%
  - Usage Guide 78 pages +24%
  - Test Cases 880 pages +70%
  - Use Cases 130 pages

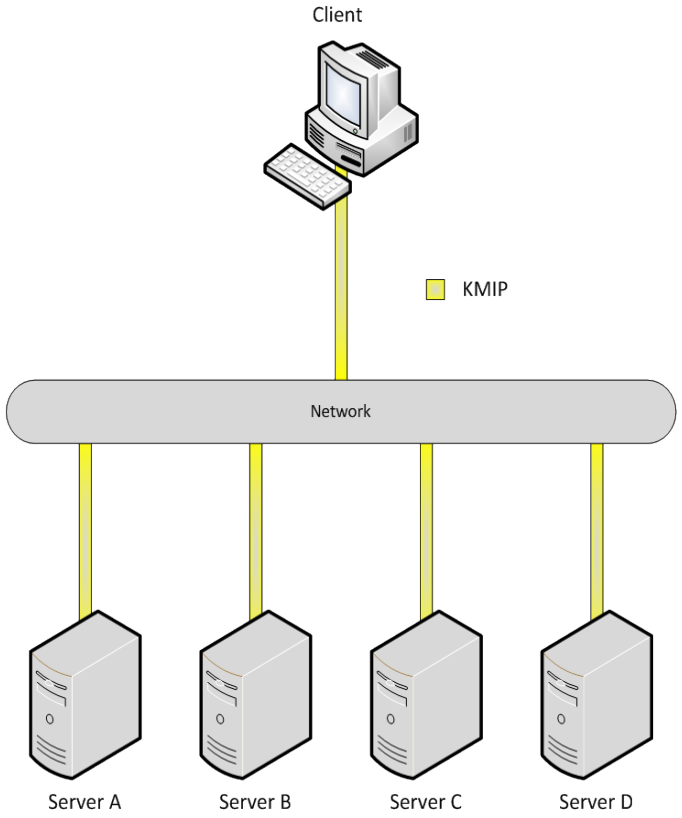
OASIS KMIP Specification

- OASIS KMIP 1.3 – PR Aug 2016, CS Aug 2016, *OS Late 2016*
  - Committee Specification Complete
  - Specification - 221 Pages; Profiles 65 Pages + XML 15,000 lines
  - OASIS Specification process underway
  - Note: Test Cases externalised into separate XML files
- OASIS KMIP 1.4 – *Early 2017*
  - Committee Working Drafts almost finalised
- OASIS KMIP 2.0 – *Started – expect late 2017/early 2018*
  - Focus of future work
  - Many items discussed over last three face to face meetings deferred for KMIP 2.0

Multi-Vendor – Single Integration



Prior to KMIP each application had to support each vendor protocol



With KMIP each application only requires support for one protocol

Multi-Vendor – Single Integration

- Positive
  - Single Integration w/ single SDK
  - Common vocabulary
  - Greater choice of technology providers
  - “Free” interoperability without point-to-point testing
- Negative
  - Must follow a standard
  - Vocabulary may not match current usage
  - May need to implement more than is strictly necessary
  - No control over end-user integration

Choice – Subset of Server Vendors

Data Security Options

- As a client (device) vendor it makes sense
  - Allow the customer to make the hard problem their own
  - Allow the customer to choose between multiple vendors to solve the hard problem
  - Enable end-customer de-provisioning/re-provisioning
  - Lower costs for you and your customer

Data Security Options

- As a server (appliance) vendor it makes sense
  - Support multiple products
  - Focus on features and capability rather than point-to-point integrations
  - Allow the customer to choose between multiple vendors
  - Customer migration enables more opportunities over the life-time of the product

Data Security Options

- Performance
  - Client rate / operation mix
- Capacity
  - Total clients / total objects
- High-availability
  - Total nodes / geographic distribution options
- Disaster Recovery
  - Backup / Recovery / Migration

Data Security Options

- Performance
  - Range from slow to fast
- Capacity
  - Range from 10’s to 10,000,000+
- High-availability
  - Range from single node to 8+ node clusters
- Disaster Recovery
  - Range from none to vendor-specific to open migration

Data Security Options

- Deployment options
  - Physical hardware appliance
  - Virtual software appliance
  - Dynamic virtual software appliance
- Security Foundation
  - Software-only
  - Software with internal Hardware
  - Software with external Hardware support

Tim Hudson

CTO @ Cryptsoft

tjh@cryptsoft.com

Thank you!

Download this presentation and others from SNIA's Data Storage Security Summit at:
http://www.snia.org/dss-summit