Enterprise Key Management & KMIP

The Real Story - Q&A with EKM Vendors

Introductions

- Moderator:
  - Tony Cox – Chair - SNIA Storage Security Industry Forum (Cryptsoft)
- Panelists:
  - Tim Hudson - CTO, Cryptsoft
  - Bob Lockhart - Chief Solutions Architect, Thales e-Security, Inc
  - Imam Sheikh - Director of Product Management, Vormetric Inc
  - Liz Townsend - Director of Business Development, Townsend Security
  - Nathan Turajski - Senior Product Manager, HP

Panelist – Tim Hudson & Cryptsoft

- CTO, Cryptsoft
- Cryptsoft EKM/KMIP Products
  - KMIP Client products:
    - KMIP Client SDKs (C, Java, C#, Python)
    - KMIP Client Layered Protocol SDKs for Proprietary Protocols
    - KMIP Adapters
    - KMIP Interoperability Test Suites
    - KMIP Cloud Online Test Service
  - KMIP Server products:
    - KMIP Server SDKs (C & Java)
    - KMIP Alert Server SDK
    - KMIP Server Administration Interface
    - KMIP C Proxy Servers for Proprietary Protocols
    - KMIP C Server Integration Modules (PKCS#11, HSM, RNG)
    - KMIP C Server OTP Server Modules

Panelist – Bob Lockhart & Thales

- Chief Solutions Architect, Thales e-Security, Inc
- Thales EKM/KMIP Products:
  - KeyAuthority 4.x

Panelist – Imam Sheikh & Vormetric

- Director of Product Management, Vormetric Inc
- Vormetric EKM/KMIP Products:
  - Data Security Manager

Panelist – Liz Townsend – Townsend Security

- Director of Business Development, Townsend Security
- Townsend Security EKM/KMIP Products
  - Alliance Key Manager

Panelist – Nathan Turajski & HP

- Senior Product Manager, HP
- HP EKM/KMIP Products:
  - Enterprise Secure Key Manager
  - ESL Tape Library Product Suite
  - MSL Tape Library Product Suite
  - MSL Tape Autoloader,
  - 3PAR StoreServ 7000,
  - 3PAR StoreServ 7450,
  - 3PAR StoreServ 10000,
  - HP XP7 DKA Encryption Software







Objectives

- Session objective 1 - Explore perspectives of Enterprise Key Management (EKM) and KMIP
- Session objective 2 – Answer questions from the floor related to EKM & KMIP

Moderator Questions - General:

1. What are the most critical customer concerns that most often come up as barriers to adoption, or which create the most conflict, when deciding to implement standards-based key management?
2. Why are standards-based approaches necessary over the proprietary implementations we've seen historically?
3. What differentiates a local key management solution vs. remote or centralized approaches—are there different scenarios that warrant something simple vs. an enterprise key management solution?

Moderator Questions - Market:

1. How do you see the rate of adoption and/or deployment of KMIP products availability?
2. What level of requirement for EKM/ KMIP do you see from the encryption key management market?
3. What are the success factors when deciding to develop a KMIP product?

Moderator Questions – Audit and Innovation:

1. How does KMIP enable greater scope for privacy and financial audits?
2. How are you taking advantage of KMIP for auditing purposes?
3. What new features and capabilities are you looking forward to in future KMIP versions
4. How have you extended existing KMIP/EKM capability outside of encryption key management?

Moderator Questions - Analysts:

- Some statements from “KMIP, KMIP, Hooray” (07/12) – Derek E. Brink - Aberdeen. Are these claims plausible?

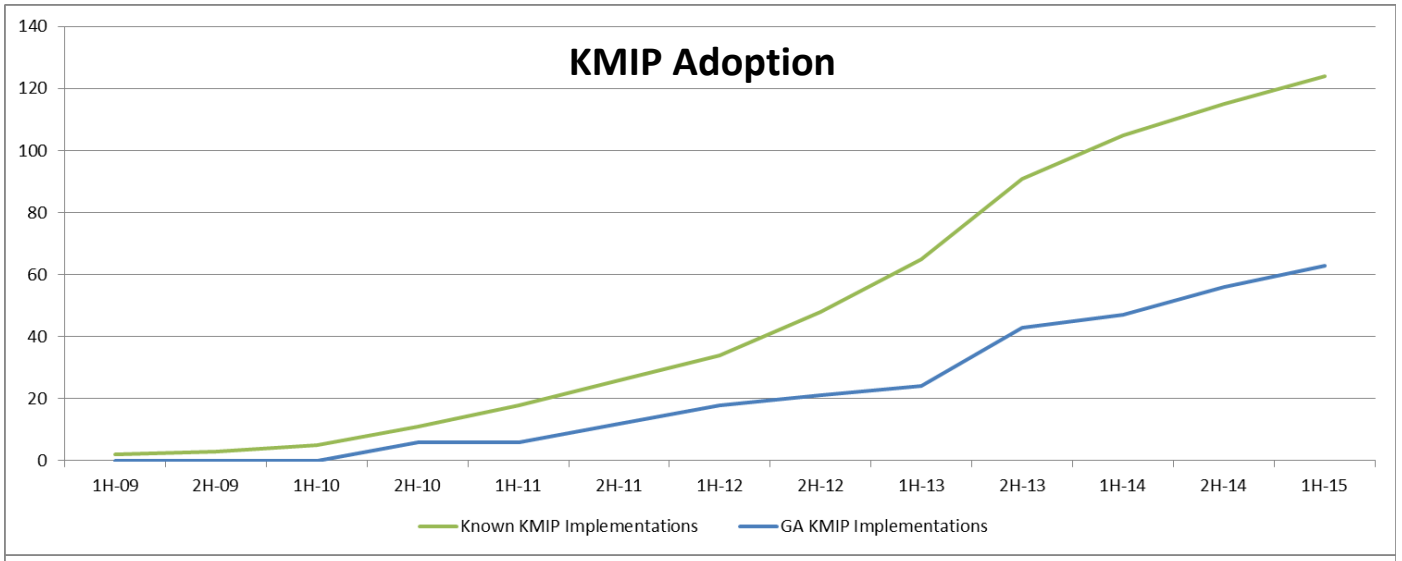
1. “Over the last 12 months, EKM users had 58% fewer security-related incidents, and 60% fewer compliance/audit deficiencies”
2. “..analysis of companies with current encryption initiatives involving enterprise key management found that the combined difference in costs avoided plus costs saved provided an advantage of nearly $100 per end-user per year over those that did not, in addition to the ability to support encryption in greater diversity and at higher scale..”

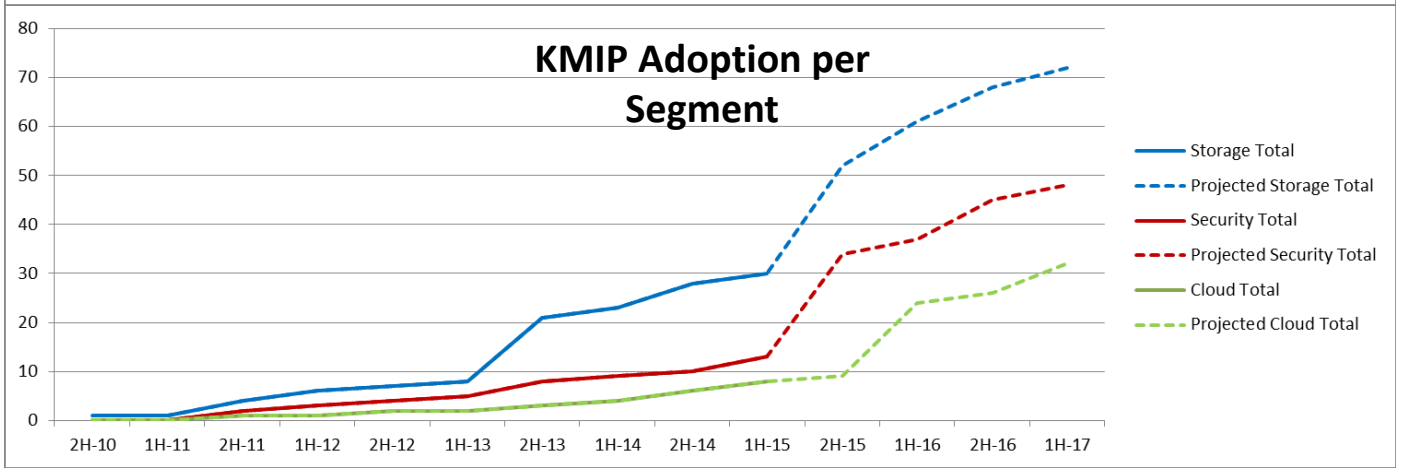
Moderator Questions - Analysts:

- Some statements from “Welcome to the New Era of Encryption” (9/10/15) – John Kindervag – Forrester. How can KMIP be a successful standard if these are true?

1. “.. it takes too long for standards to be created. There are also significant compromises between various parties that are necessary to bring a standard to life. ..”
2. “Many standards will be outdated before industry bodies can even release them. Given the rate of change in technology today, standards lag.”
3. “Vendors want freedom to disrupt and innovate. Standards often inhibit innovation.”
4. “Legacy vendors dominate standards bodies. The standards bodies are typically stacked with participants from older, established companies.”

KMIP Adoption





Source - Cryptsoft

Storage

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

Security & Infrastructure

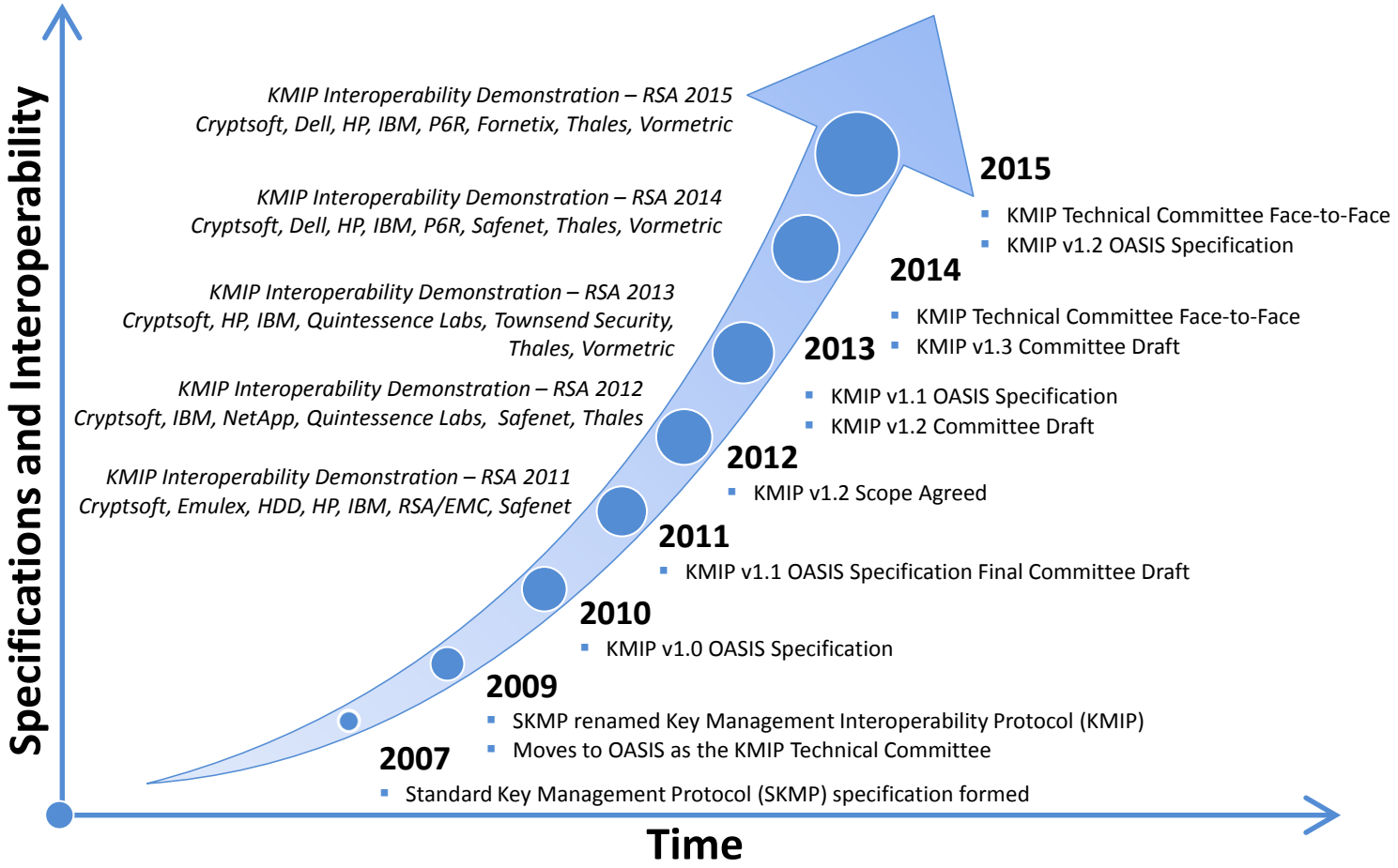
- Key Managers
- Hardware security modules
- Encryption Gateways
- Virtualization Managers
- Virtual Storage Controllers
- Virtual Network Appliances

Cloud

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

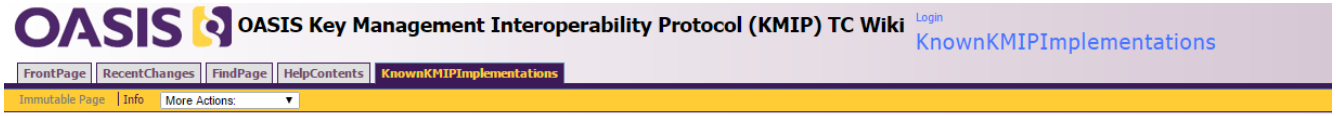
Source - Cryptsoft

KMIP Specification Development



Source - Cryptsoft

Known KMIP Implementations



KMIP Implementations known to the KMIP TC

NOTE: The Following list of known KMIP implementations that have been brought to the attention of the OASIS KMIP Technical Committee.

The KMIP TC in no way endorses these implementations nor does it make any statements as to the suitability, quality, availability or level of conformance to the KMIP Specification or Test Cases.

This list is provided as a repository for the convenience of OASIS TC Members and parties interested in the adoption of interoperable key management.

For product conformance please refer to the KMIP Conformance Program offered by SNIA SSIF (http://www.snia.org/forums/SSIF/kmip).

KMIP Implementations - OASIS Interoperability Tested or Conformance Tested

NOTE: The following implementations have participated in OASIS Interoperability Tests or Conformance Testing noted below.
-Implementations are identified according to the applicable test documentation.
-This list is moderated by the KMIP Interoperability Subcommittee Chair.

Company	Name	Interop (year)	Conformance Tested
Cryptsoft	KMIP C Client SDK	2011, 2012, 2013, 2014	Jan 2015
Cryptsoft	KMIP Java Client SDK	2011, 2012, 2013, 2014	
Cryptsoft	KMIP CSharp Client SDK	2012, 2013, 2014	
Cryptsoft	KMIP Python Client SDK	2014	
Cryptsoft	KMIP C Server SDK	2011, 2012, 2013, 2014	Nov 2014
Cryptsoft	KMIP JavaServer SDK	2011, 2012, 2013, 2014	
Dell	Dell Data Protection Server	2014	
HP	Enterprise Secure Key Manager	2012, 2013, 2014	Nov 2014
HP	MSL Tape Library	2014	
HP	StoreEver MSL6480 Tape Library		Jul 2015
IBM	Research Server	2010, 2011	
IBM	Tivoli Key Lifecycle Manager	2012, 2013	
IBM	Security Key Lifecycle Manager	2014	
NetApp	NetApp Storage Encryption	2012	
P6R	Secure KMIP Client (SKC) SDK	2014	
QuintessenceLabs	QKM - Client	2012, 2013	
QuintessenceLabs	QKM	2012, 2013	
SafeNet	KeySecure	2011, 2012, 2014	
Thales e-Security	keyAuthority	2012, 2013, 2014	
Vormetric	Data Security Manager	2013, 2014	

Source - https://wiki.oasis-open.org/kmip/KnownKMIPImplementations

Known KMIP Implementations

Commercially Available KMIP Products

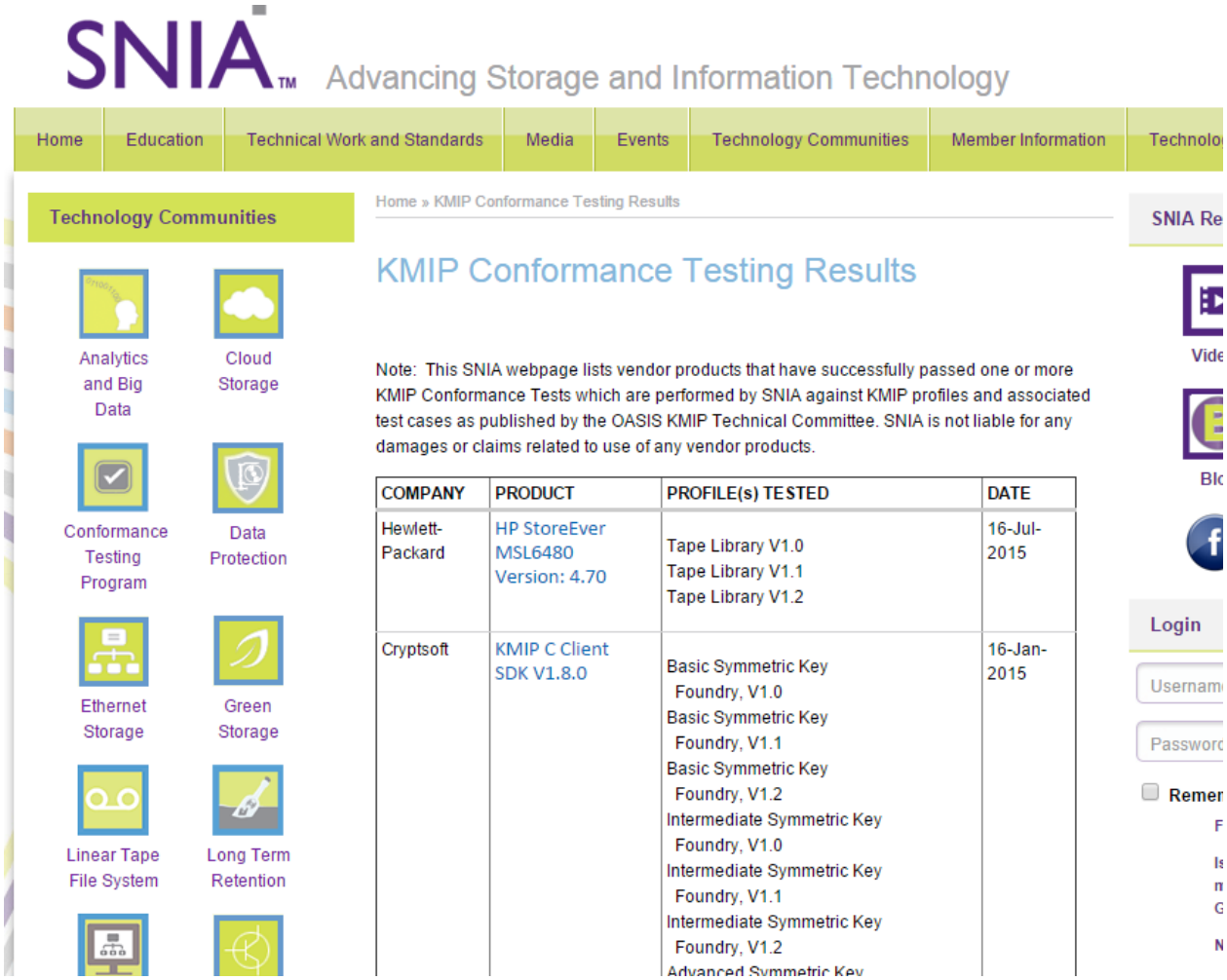
NOTE: As a general guide, an implementations noted as Commercially Available KMIP Product is included if:
- it is generally available for sale with **claimed** KMIP support and noted on a vendor web page as such; **or**
- an OASIS KMIP TC member can publicly state that some form of KMIP conformance has been verified.

The level of claimed conformance for any implementation should be verified independently or refer to the SNIA SSIF KMIP Conformance Program noted above.

Company	Name
BDT Media Automation	Tape Libraries
Bloombase	KeyCastle, StoreSafe, Spitfire Message
Brocade	Encryption SAN Switch
Ciphercloud	Discover, Protect and Monitor Platform
Cryptsoft	KMIP C Client SDK, KMIP Java Client SDK, KMIP CSharp Client SDK, KMIP Python Client SDK, KMIP C Server SDK, KMIP Java Server SDK
DataStax	DataStax Enterprise, DataStax OpsCenter
Dell	Dell Compellent Storage Center Series
Fujitsu	Eternus-SF KM
Gazzang	Gazzang zTrustee
Hitachi	HUS 150, HUS VM, VSP
HP	Enterprise Secure Key Manager, ESL Tape Library, MSL Tape Library, MSL Tape Autoloader, 3PAR StoreServ 7000, 3PAR StoreServ 7450, 3PAR StoreServ 10000, HP XP7 DKA Encryption Software
IBM	XIV Storage Systems 114 and 214, Security Key Lifecycle Manager
Liason Technologies	Encryption Key Manager
Luminex	CGSafe
NetApp	NetApp Storage Encryption
Netskope	Netskope Active
Oracle	Oracle Key Vault
P6R	Secure KMIP Client (SKC) SDK
Panzura	Quicksilver Cloud Storage Controller
Perspecsys	Cloud Data Protection Gateway
Quantum	Scalar i6000, Scalar i500, Scalar i80, Scalar i40
QuintessenceLabs	qCrypt Key Manager, qCrypt-xStream Key Manager with Quantum RNG, qClient KMIP SDK, qVZ Virtual Zeroisation Storage System
RSA	Data Protection Manager
SafeNet	KeySecure
Sepaton	S2100-ES3 Data Protection Appliance
ServiceMesh	Agility Platform
Skyhigh Networks	Skyhigh Secure
Thales e-Security	keyAuthority
Townsend Security	Alliance Key Manager
Trend Micro	SecureCloud
Venafi	Trust Protection Platform
Vormetric	Data Security Manager

Source - https://wiki.oasis-open.org/kmip/KnownKMIPImplementations

SSIF KMIP Conformance Testing



Thank you

- Thank you to:
  - Panelists:
    - Tim Hudson
    - Bob Lockhart
    - Imam Sheikh
    - Liz Townsend
    - Nathan Turajski
  - SNIA & SSIF
  - Summit Underwriters and Sponsors