Standardised Encryption Key Management for Smart Grids with KMIP

Tony Cox

VP, Partners, Alliances & Standards - Cryptsoft
tony.cox@cryptsoft.com

CRYPTSOFT

Introduction – Tony Cox

CRYPTSOFT

- VP Partners, Alliances & Standards

OASIS

- Co-Chair KMIP Technical Committee
- Co-Author KMIP Specification (v1.3, v1.4, v2.0)
- Co-Chair PKCS#11 Technical Committee

Cryptsoft

- Established in 1996
- Privately owned
- Australian based OEM security technology supplier
- ISO 9001 quality assured company

BDT BRACKET COMPUTING CSC DATASTAX DELL DELLEMC

ETINET FORNETIX Hewlett Packard Enterprise HUAWEI HYTRUST Cloud Under Control

InterSystems Health | Business | Government ISKRAEMECO MarkLogic NetApp netskope

nimble storage a Hewlett Packard Enterprise company panzura PLURIBUS NETWORKS reduxio rsd Your Information. Governed. SEPATON

SNIA SPECTRA THALES TREND MICRO Vormetric

CRYPTSOFT

OASIS

- OASIS is a nonprofit consortium that drives the development, convergence and adoption of open standards for the global information society.
- Established in 1993 as SGML Open (“Standardised General Markup Lanugauge”)
- Changed to OASIS in 1998 with expanded scope as “Organization for the Advancement of Structured Information Standards”
- Over 100 standards completed and in use
- Over 60 active Technical Committees
- Links to other standards bodies including ISO for standards publication

OASIS Membership

- 3 Member levels
  - Foundational Sponsor
  - Sponsor Member
  - Contributor Member
- Foundational Sponsors

CRYPTSOFT IBM Microsoft

- Over 65 Sponsor members
- Over 195 Contributor members
- Well established Technical Committee processes
- Formal, structured standards publication & review process

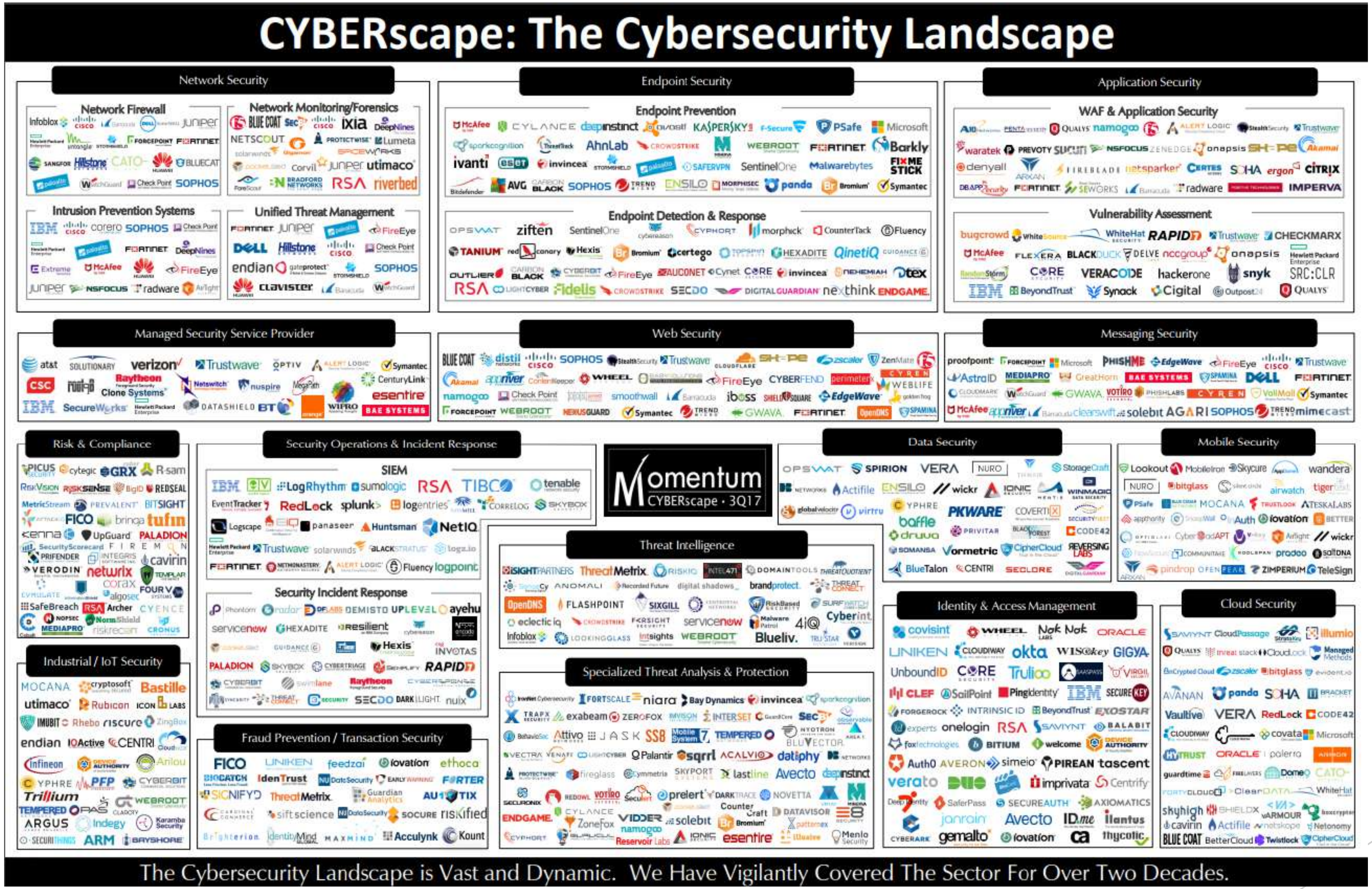
Overview

- Cybersecurity Landscape
- Keys & Certificates in a Smart Grid System
- Key and Certificate Management
- Key Management History
- KMIP – Overview and History
- KMIP – Profiles & Testing
- KMIP & Smart Grid

Cybersecurity Landscape

CRYPTSOFT

Cybersecurity context


CYBERscape: The Cybersecurity Landscape
Network Security
Network Firewall
Network Monitoring/Forensics
Intrusion Prevention Systems
Unified Threat Management
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Vulnerability Assessment
Managed Security Service Provider
Web Security
Messaging Security
Risk & Compliance
Security Operations & Incident Response
SIEM
Security Incident Response
Momentum CYBERscape · 3Q17
Threat Intelligence
Data Security
Mobile Security
Industrial / IoT Security
Fraud Prevention / Transaction Security
Specialized Threat Analysis & Protection
Identity & Access Management
Cloud Security
The Cybersecurity Landscape is Vast and Dynamic. We Have Vigilantly Covered The Sector For Over Two Decades.

CRYPTSOFT

* Source: Momentum Partners

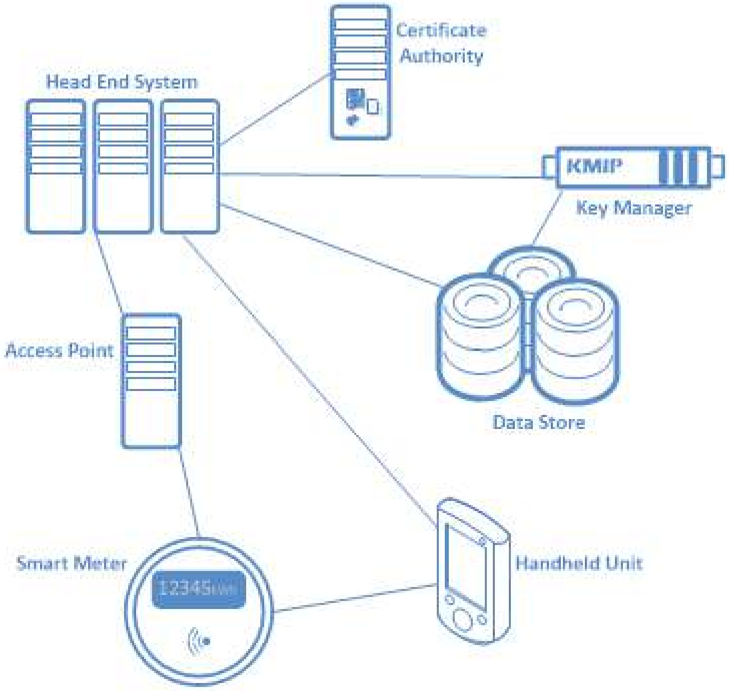
Cybersecurity context

- 5 main Areas of focus
  - Identification
  - Protection
  - Detection
  - Response
  - Recovery
- Focus on protection:
  - Assets
  - Information
  - Authentication & Encryption

Keys and Certificates in Smart Grid Systems

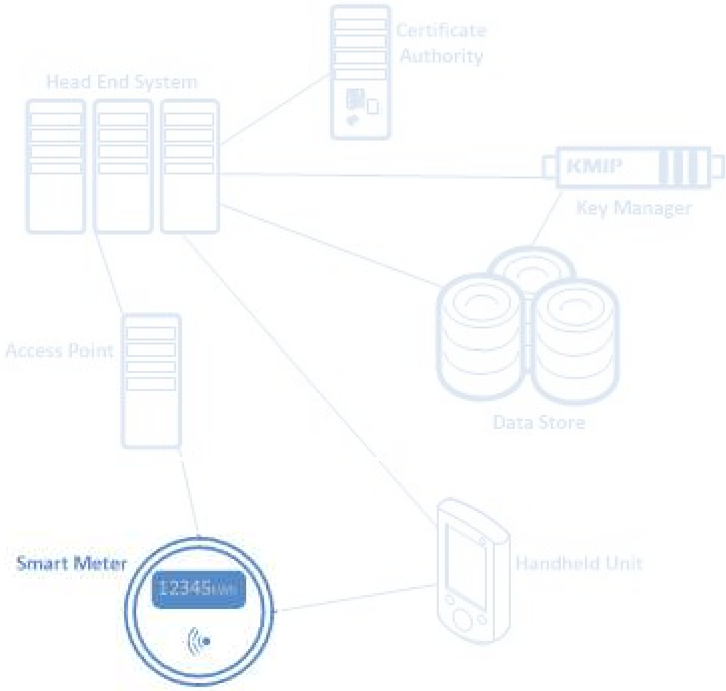
Keys & Certificates in a Smart Grid System

- Major components
  - Smart Meters
  - Access Points
  - Handheld Units
  - Head End Systems
  - Data Stores
  - Key Management System



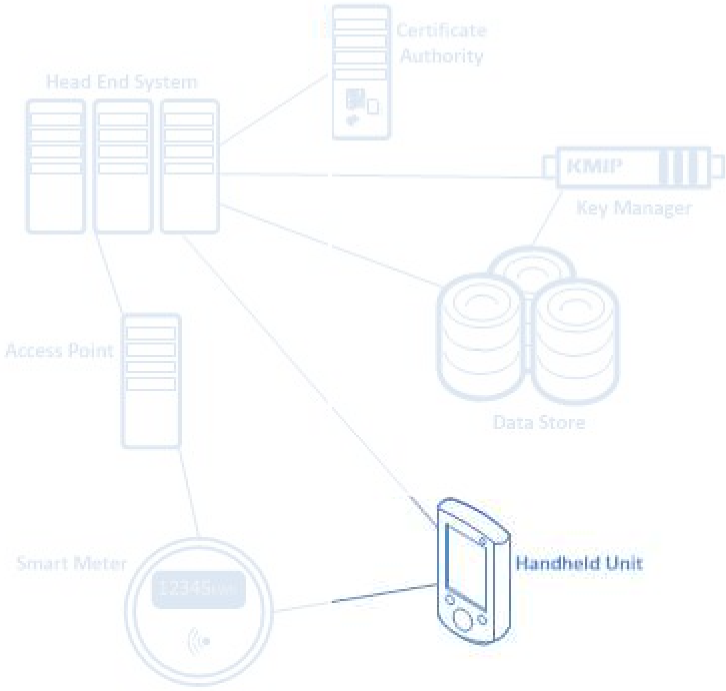
Keys & Certificates in a Smart Grid System

- Smart meters
  - Manufacturer Keys & Certificates
  - Operator encryption keys
  - Authentication keys & certificates
  - Generally 5-12 Security Objects



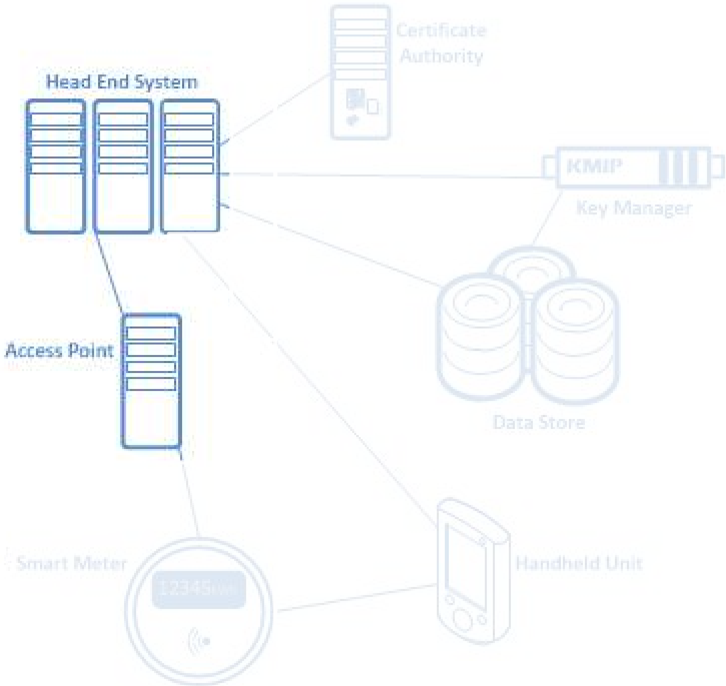
Keys & Certificates in a Smart Grid System

- Hand Held Unit
  - Manufacturer Keys & Certificates
  - Operator encryption keys
  - Authentication keys & certificates
  - Variable number of Security Objects



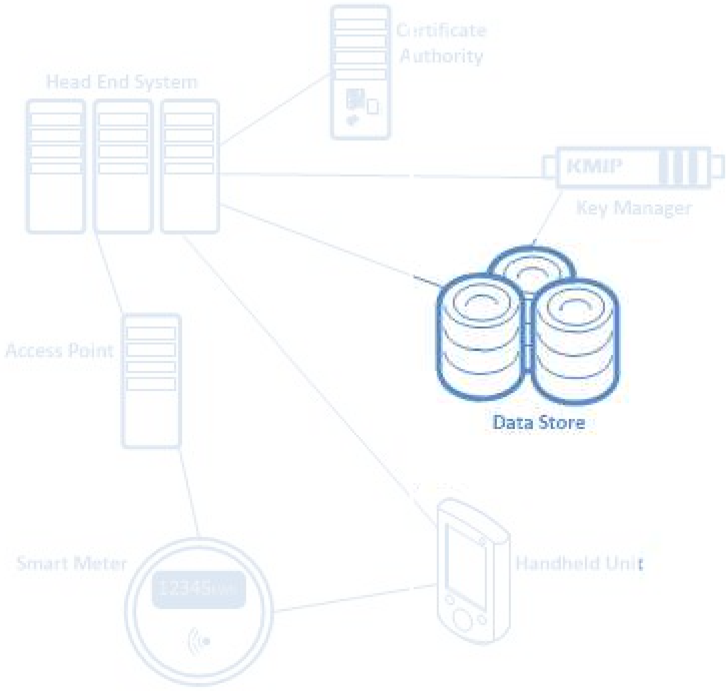
Keys & Certificates in a Smart Grid System

- Access Point & Head End Systems
  - Manufacturer Keys & Certificates
  - Operator encryption keys
  - Authentication keys & certificates
  - Large number of Security Objects



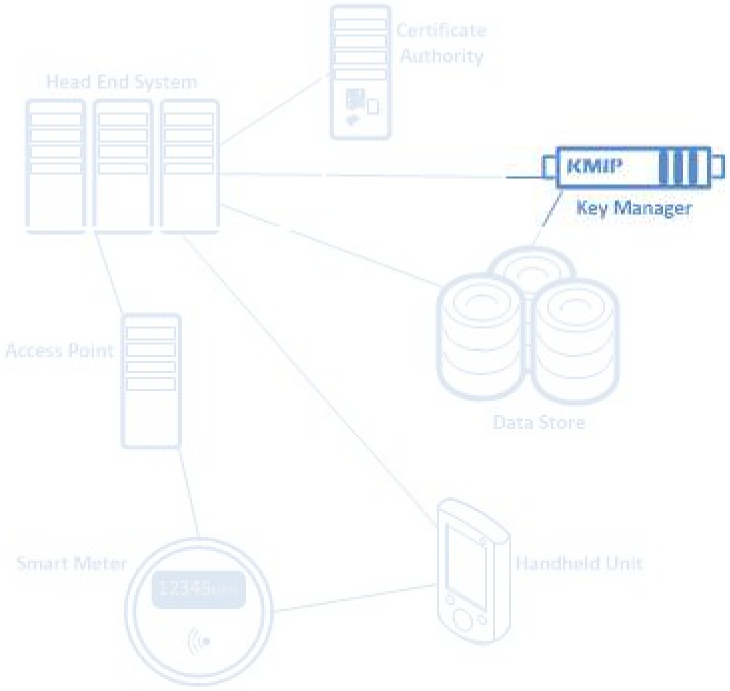
Keys & Certificates in a Smart Grid System

- Data Store
  - Data encryption keys
  - Operator encryption keys
  - Authentication keys & certificates
  - Very large number of Security Objects



Keys & Certificates in a Smart Grid System

- Key Management System requirements
  - Capacity to store $10^{e}6$ to $10^{e}8$ of Security objects
  - Full lifecycle management
  - Multiple, discrete partitions or domains
  - Usually offer redundancy & high availability via multi-node replicating clusters



CRYPTSOFT

Key and Certificate Management

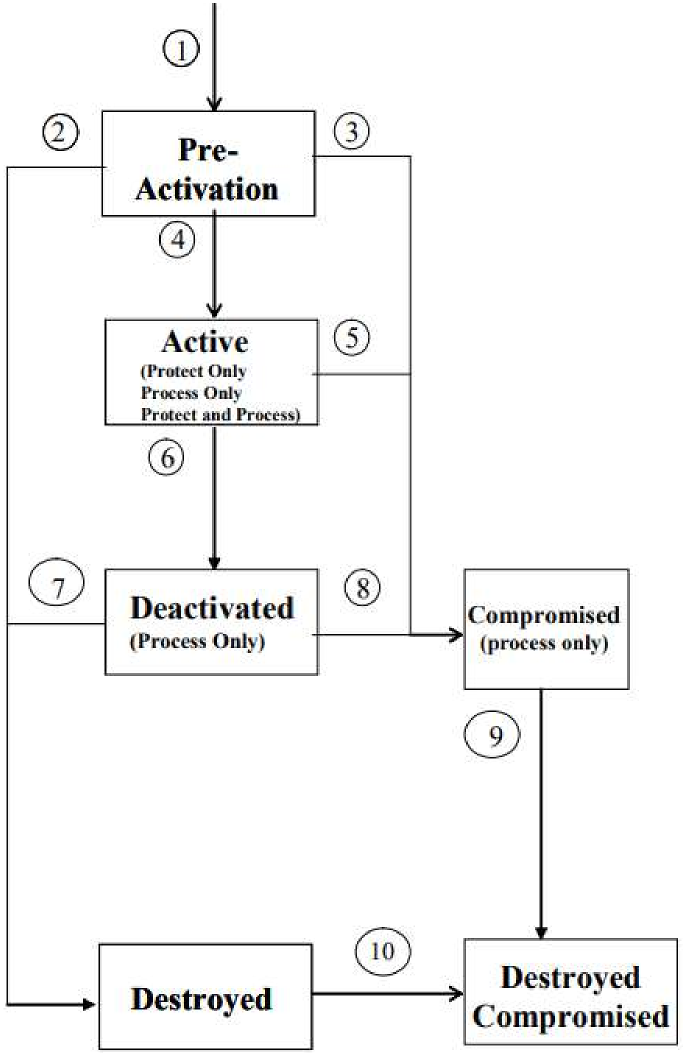
Key and Certificate Management

- Lifecycle
  - Provisioning
  - Use
  - Deprovisioning
  - Standards
- Metadata associated with:
  - lifecycle events
  - Data
  - System
  - User
  - Authority

CRYPTSOFT

Key and Certificate Management

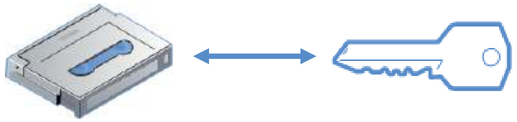
- NIST Special Publication 800-57 Pt 1 (r1-2005)
- States
  - Pre-Activation
  - Active
  - Deactivated
  - Destroyed
  - Compromised
  - Destroyed Compromised

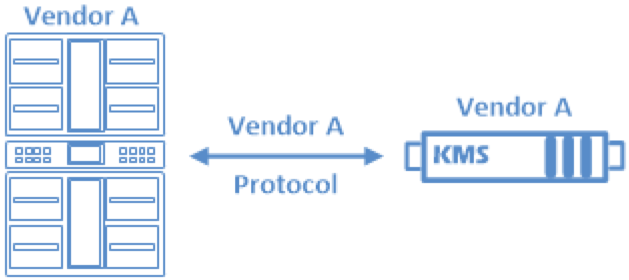


Source: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

Key Management History

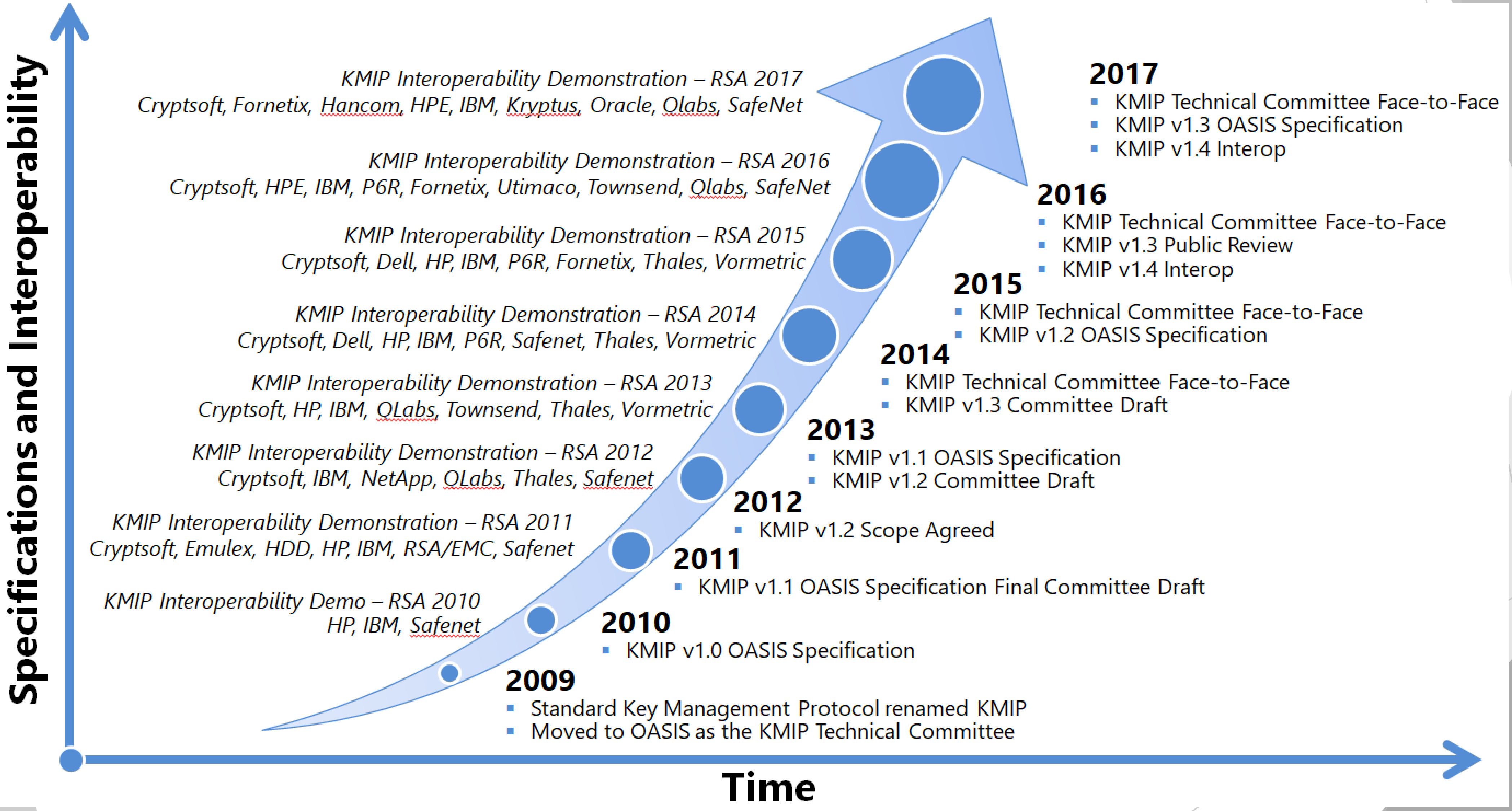
- Started with data storage (tape)
  - Key per tape
  - Key per file later
- Vendor proprietary protocols
  - Decrypt & re-encrypt on change of vendor
  - Changing vendors was costly and difficult
- Push for standardisation
  - Started by one vendor





KMIP – History & Overview

KMIP Timeline



Specifications and Interoperability

KMIP Interoperability Demonstration – RSA 2017
Cryptsoft, Fornetix, Hancom, HPE, IBM, Kryptus, Oracle, Qlabs, SafeNet

KMIP Interoperability Demonstration – RSA 2016
Cryptsoft, HPE, IBM, P6R, Fornetix, Utimaco, Townsend, Qlabs, SafeNet

KMIP Interoperability Demonstration – RSA 2015
Cryptsoft, Dell, HP, IBM, P6R, Fornetix, Thales, Vormetric

KMIP Interoperability Demonstration – RSA 2014
Cryptsoft, Dell, HP, IBM, P6R, Safenet, Thales, Vormetric

KMIP Interoperability Demonstration – RSA 2013
Cryptsoft, HP, IBM, QLabs, Townsend, Thales, Vormetric

KMIP Interoperability Demonstration – RSA 2012
Cryptsoft, IBM, NetApp, QLabs, Thales, Safenet

KMIP Interoperability Demonstration – RSA 2011
Cryptsoft, Emulex, HDD, HP, IBM, RSA/EMC, Safenet

KMIP Interoperability Demo – RSA 2010
HP, IBM, Safenet

2017
- KMIP Technical Committee Face-to-Face
- KMIP v1.3 OASIS Specification
- KMIP v1.4 Interop

2016
- KMIP Technical Committee Face-to-Face
- KMIP v1.3 Public Review
- KMIP v1.4 Interop

2015
- KMIP Technical Committee Face-to-Face
- KMIP v1.2 OASIS Specification

2014
- KMIP Technical Committee Face-to-Face
- KMIP v1.3 Committee Draft

2013
- KMIP v1.1 OASIS Specification
- KMIP v1.2 Committee Draft

2012
- KMIP v1.2 Scope Agreed

2011
- KMIP v1.1 OASIS Specification Final Committee Draft

2010
- KMIP v1.0 OASIS Specification

2009
- Standard Key Management Protocol renamed KMIP
- Moved to OASIS as the KMIP Technical Committee

Time

* Source: Cryptsoft

KMIP Product Types

Storage

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

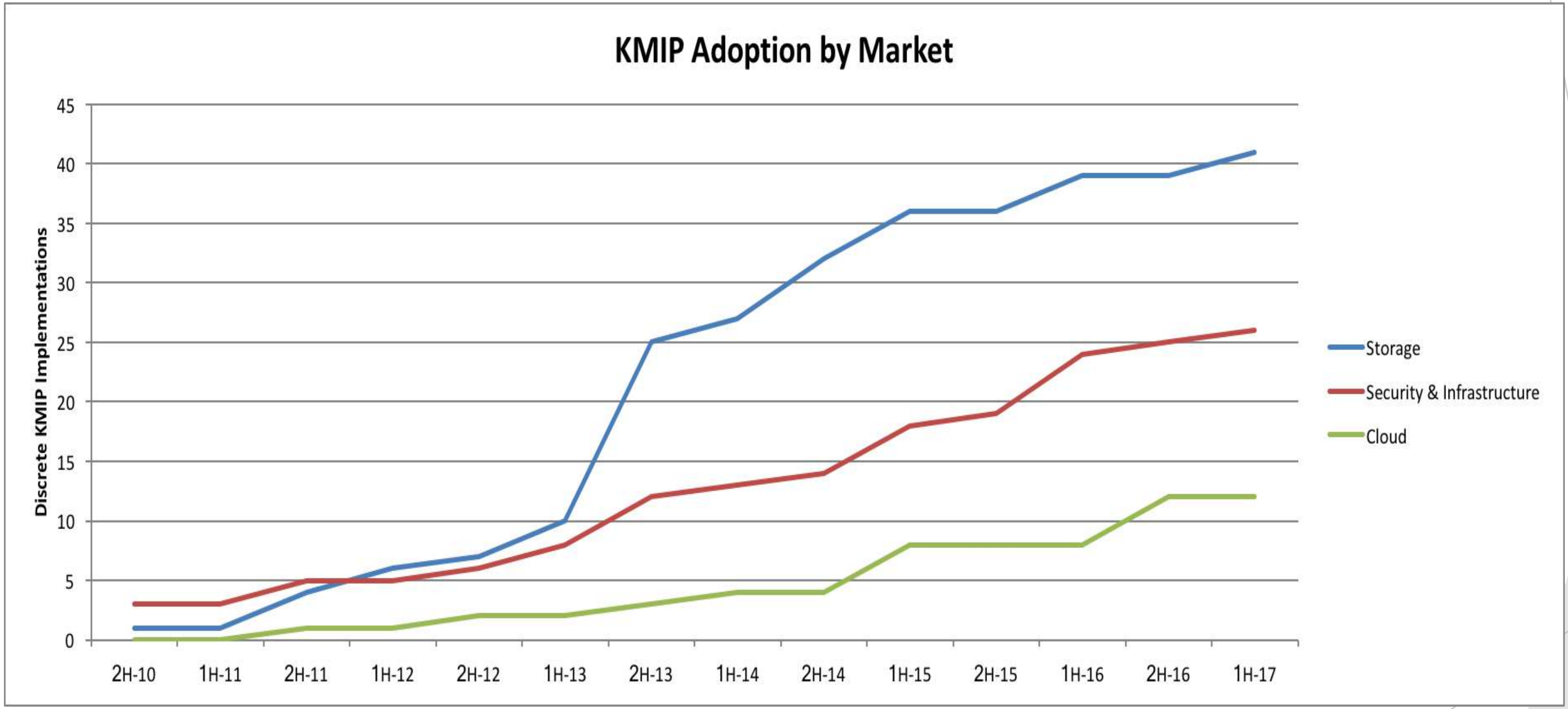
Infrastructure and Security

Key Managers & HSMs
Databases
Encryption Gateways
Virtualization Managers
Virtual Storage Controllers
Network Computing Appliances
Critical Infrastructure

Cloud and IoT

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

KMIP Growth



KMIP Adoption by Market
Discrete KMIP Implementations
45
40
35
30
25
20
15
10
5
0
2H-10
1H-11
2H-11
1H-12
2H-12
1H-13
2H-13
1H-14
2H-14
1H-15
2H-15
1H-16
2H-16
1H-17
Storage
Security & Infrastructure
Cloud

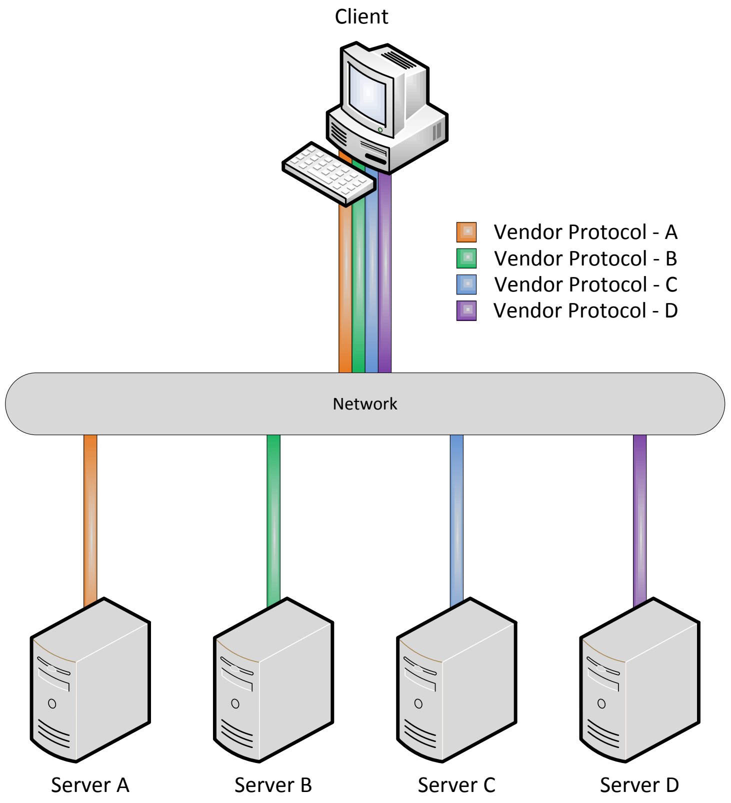
KMIP Vendors

BDT
BLOOMBASE
BRACKET COMPUTING
BROCADE
CipherCloud Trust in the Cloud
CRYPTSOFT
CSC
DATASTAX
DELL EMC
ETINET
FORNETIX
FUJITSU
HANCOM HANCOM SECURE
Hewlett Packard Enterprise
Hitachi Data Systems
HUAWEI
HYTRUST Cloud Under Control
IBM
InterSystems Health | Business | Government
ISKRAEMECO
kryptus
MarkLogic
mongoDB
NetApp
netskope
ORACLE
panzura
PLURIBUS NETWORKS
Quantum
RSA The Security Division of EMC
reduxio
rsd Your Information. Governed.
rubrik
SafeNet
SEPATON
skyhigh
SPECTRA
THALES
Townsend SECURITY
TREND MICRO
VENAFI
vmware
Vormetric
Zettaset The Leader in Big Data Security

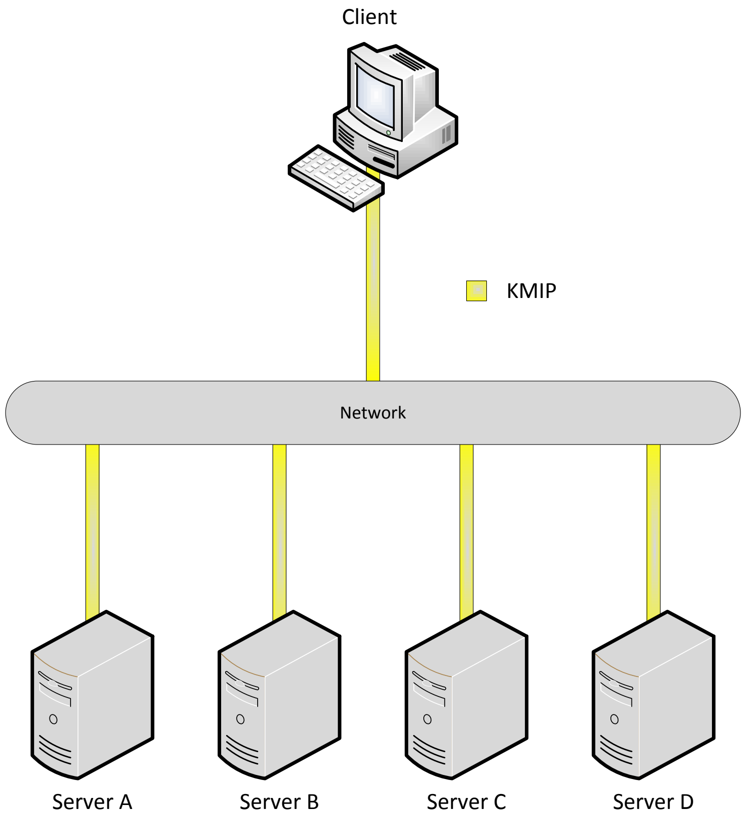
CRYPTSOFT

* Source: Cryptsoft

KMIP 101



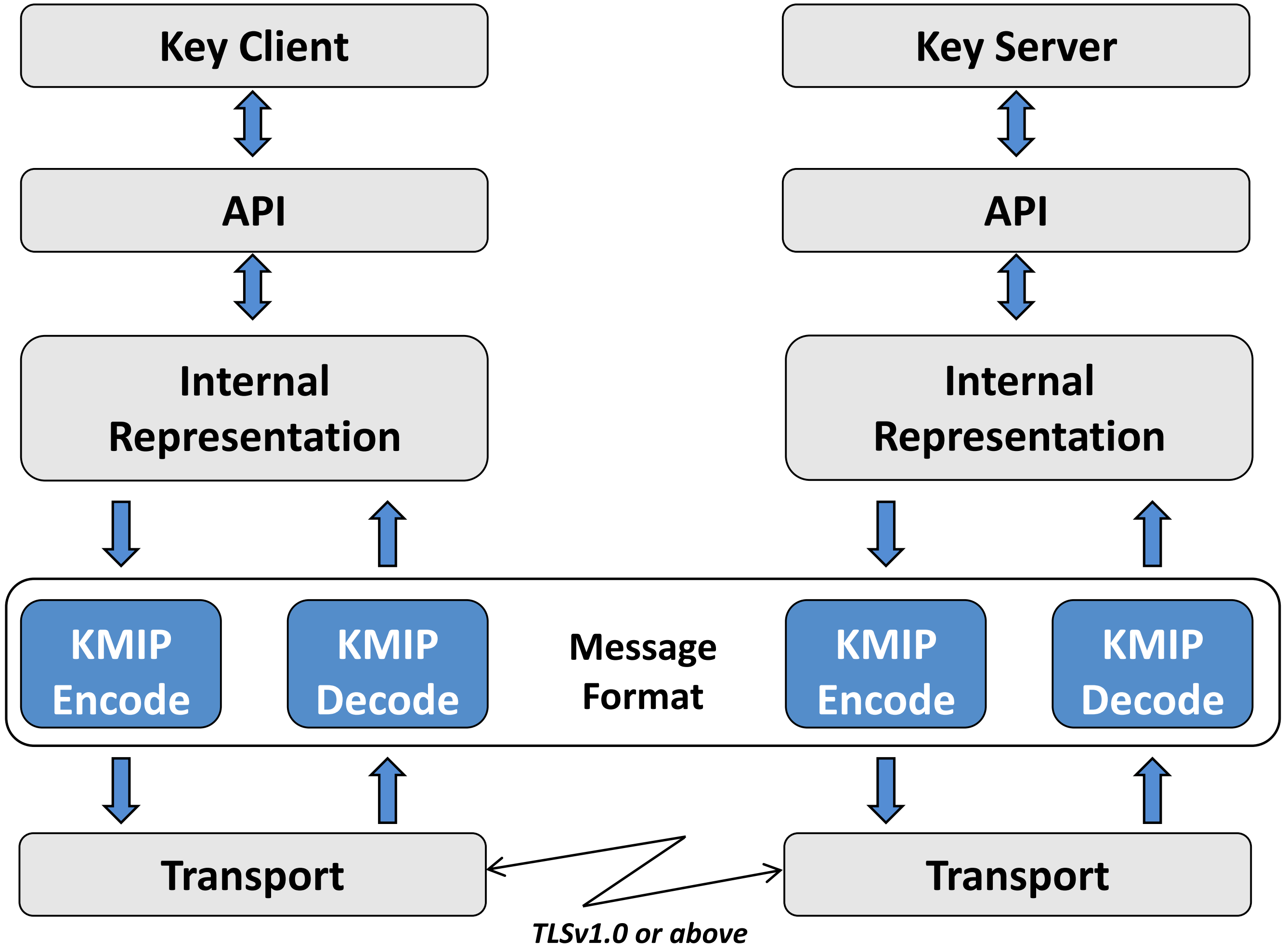
Prior to KMIP each application had to support each vendor protocol



With KMIP each application only requires support for one protocol

* Source: Cryptsoft

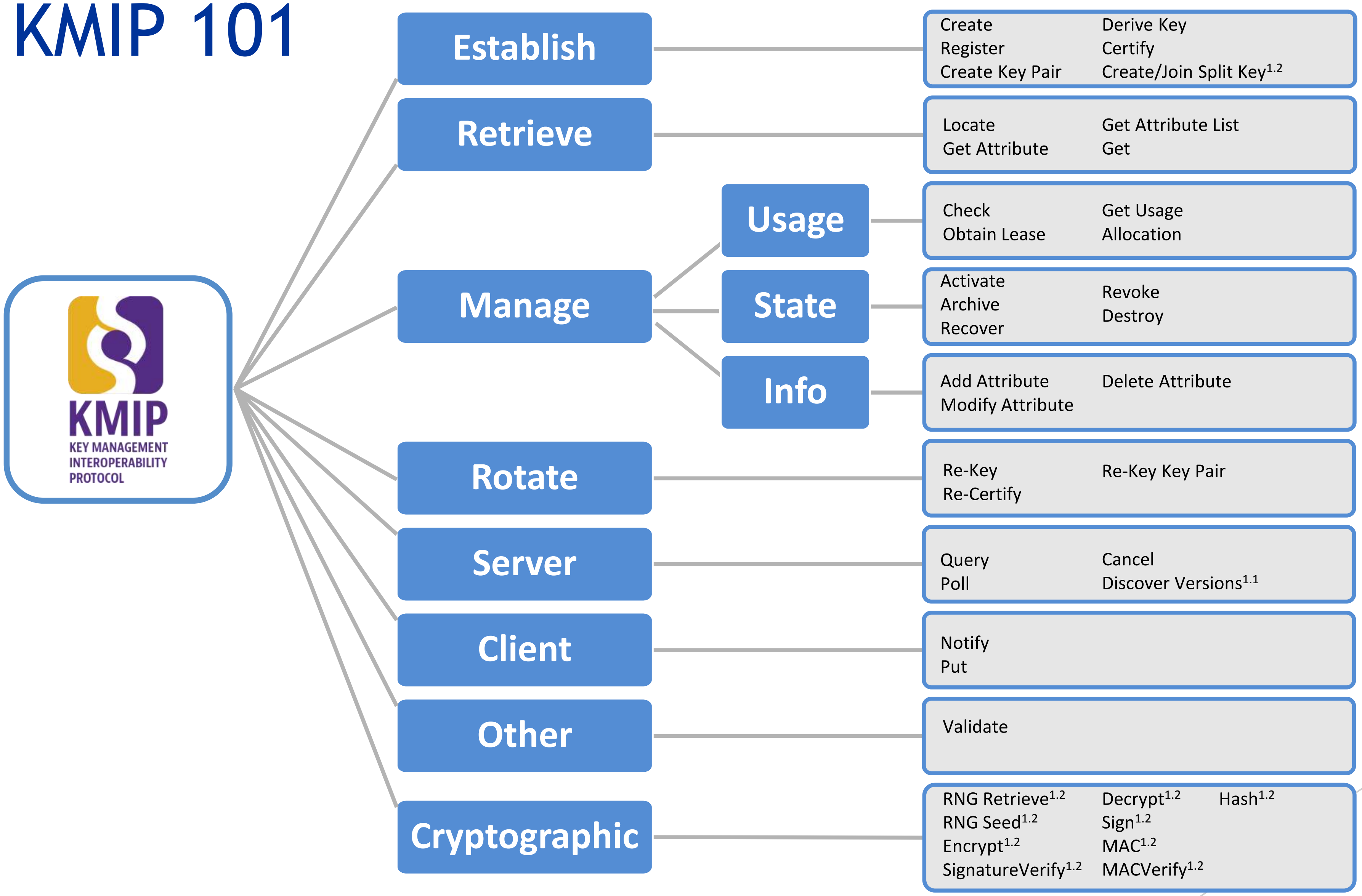
KMIP 101



CRYPTSOFT

* Source: Cryptsoft

KMIP 101



Establish
- Create
- Register
- Create Key Pair
- Derive Key
- Certify
- Create/Join Split Key$^{1.2}$

Retrieve
- Locate
- Get Attribute
- Get Attribute List
- Get

Manage

Usage
- Check
- Obtain Lease
- Get Usage
- Allocation

State
- Activate
- Archive
- Recover
- Revoke
- Destroy

Info
- Add Attribute
- Modify Attribute
- Delete Attribute

Rotate
- Re-Key
- Re-Certify
- Re-Key Key Pair

Server
- Query
- Poll
- Cancel
- Discover Versions$^{1.1}$

Client
- Notify
- Put

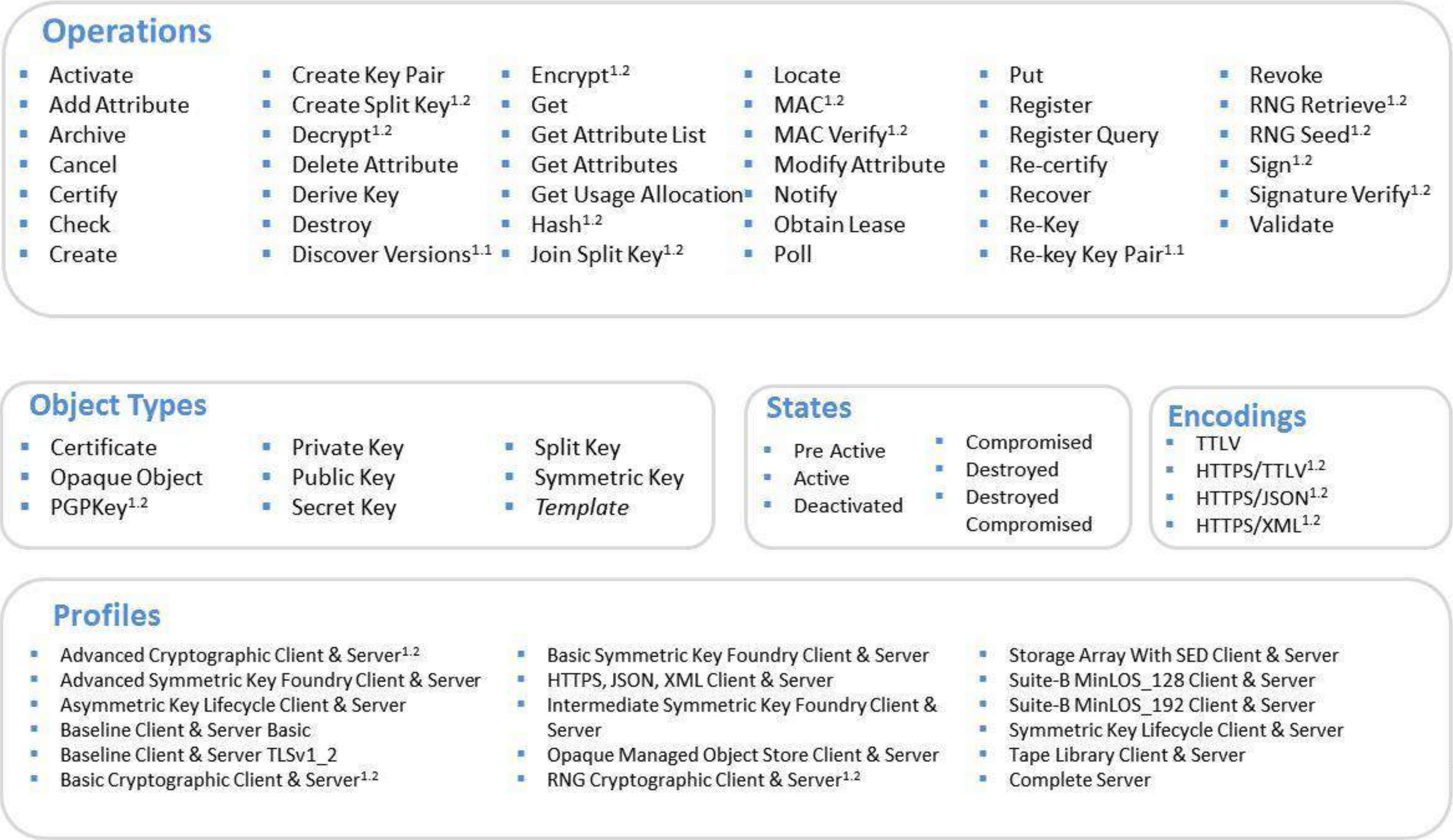
Other
- Validate

Cryptographic
- RNG Retrieve$^{1.2}$
- RNG Seed$^{1.2}$
- Encrypt$^{1.2}$
- SignatureVerify$^{1.2}$
- Decrypt$^{1.2}$
- Sign$^{1.2}$
- MAC$^{1.2}$
- MACVerify$^{1.2}$
- Hash$^{1.2}$

CRYPTSOFT

* Source: Cryptsoft

KMIP 101



Operations

- Activate
- Add Attribute
- Archive
- Cancel
- Certify
- Check
- Create
- Create Key Pair
- Create Split Key$^{1.2}$
- Decrypt$^{1.2}$
- Delete Attribute
- Derive Key
- Destroy
- Discover Versions$^{1.1}$
- Encrypt$^{1.2}$
- Get
- Get Attribute List
- Get Attributes
- Get Usage Allocation
- Hash$^{1.2}$
- Join Split Key$^{1.2}$
- Locate
- MAC$^{1.2}$
- MAC Verify$^{1.2}$
- Modify Attribute
- Notify
- Obtain Lease
- Poll
- Put
- Register
- Register Query
- Re-certify
- Recover
- Re-Key
- Re-key Key Pair$^{1.1}$
- Revoke
- RNG Retrieve$^{1.2}$
- RNG Seed$^{1.2}$
- Sign$^{1.2}$
- Signature Verify$^{1.2}$
- Validate

Object Types

- Certificate
- Opaque Object
- PGPKey$^{1.2}$
- Private Key
- Public Key
- Secret Key
- Split Key
- Symmetric Key
- *Template*

States

- Pre Active
- Active
- Deactivated
- Compromised
- Destroyed
- Destroyed Compromised

Encodings

- TTLV
- HTTPS/TTLV$^{1.2}$
- HTTPS/JSON$^{1.2}$
- HTTPS/XML$^{1.2}$

Profiles

- Advanced Cryptographic Client & Server$^{1.2}$
- Advanced Symmetric Key Foundry Client & Server
- Asymmetric Key Lifecycle Client & Server
- Baseline Client & Server Basic
- Baseline Client & Server TLSv1_2
- Basic Cryptographic Client & Server$^{1.2}$
- Basic Symmetric Key Foundry Client & Server
- HTTPS, JSON, XML Client & Server
- Intermediate Symmetric Key Foundry Client & Server
- Opaque Managed Object Store Client & Server
- RNG Cryptographic Client & Server$^{1.2}$
- Storage Array With SED Client & Server
- Suite-B MinLOS_128 Client & Server
- Suite-B MinLOS_192 Client & Server
- Symmetric Key Lifecycle Client & Server
- Tape Library Client & Server
- Complete Server

CRYPTSOFT

* Source: Cryptsoft

KMIP 101

Ver	Specification Status	Market Status	Main Features
v1.2	Published May 2015	• Widely deployed • Many customer utilising the enhanced capability and interoperability • Deployed to SNIA SSIF conformance testing program (using Cryptsoft Test Suite) • Multiple vendors through formal testing program	• Cryptographic Services • Profiles expansion • Suite B support • Additional Interoperability Updates
v1.3	Published December 2016	• Expanded deployment • Deployment to SNIA SSIF conformance testing program (using Cryptsoft Test Suite) in Q3-2016 • Multiple products interop tested & demonstrated at RSA Conference 2015.	• Suite B updates • Automated client registration • Limited deprecations • Additional Cryptographic Services
v1.4	Undergoing final public review Target publication November 2017	• Initial deployments expanding • Automation and scalability benefits driving faster adoption • Multiple products interop tested & demonstrated at RSA Conference 2016.	• Automated client registration enhancements • Additional profiles • PKCS#12 handling • Further deprecations • Additional Interoperability Updates
v2.0	Drafting underway Target publication Q1 - 2018	• Technical members gathering and analysing specific demands from the market and finalising scope	• Deprecated items removed • Fine-grained attribute-based access control • Alternate protocol and message handling • Post-Quantum Computing measures

CRYPTSOFT

* Source: Cryptsoft

KMIP – Profiles and Testing

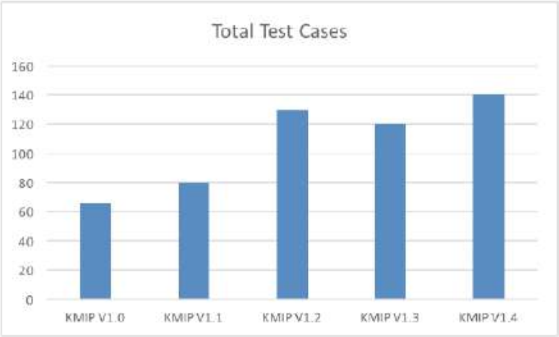
KMIP Profiles

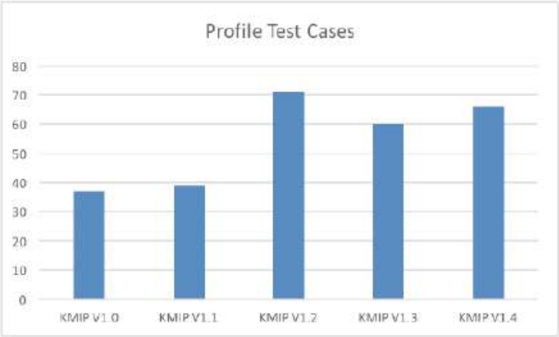
- Profiles outline a mandatory (with some allowed variation) set of conformance requirements.
- Requirements are usually a subset of specific operations, attributes and other items combined with one or more request/response traces.
- Over 100 discrete profiles for clients and servers including:
  - Tape Library
  - Storage Array with SED
  - Suite B
  - Cryptographic Services
  - Opaque Managed Object Store
- A range of new profiles under construction

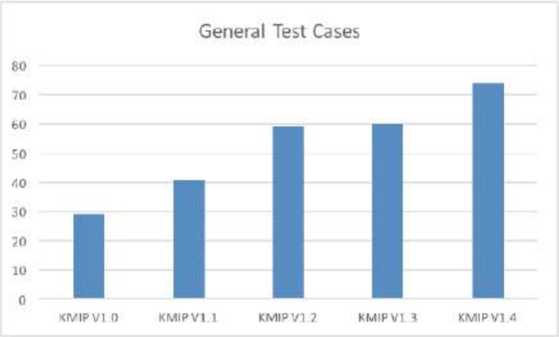
KMIP Profiles

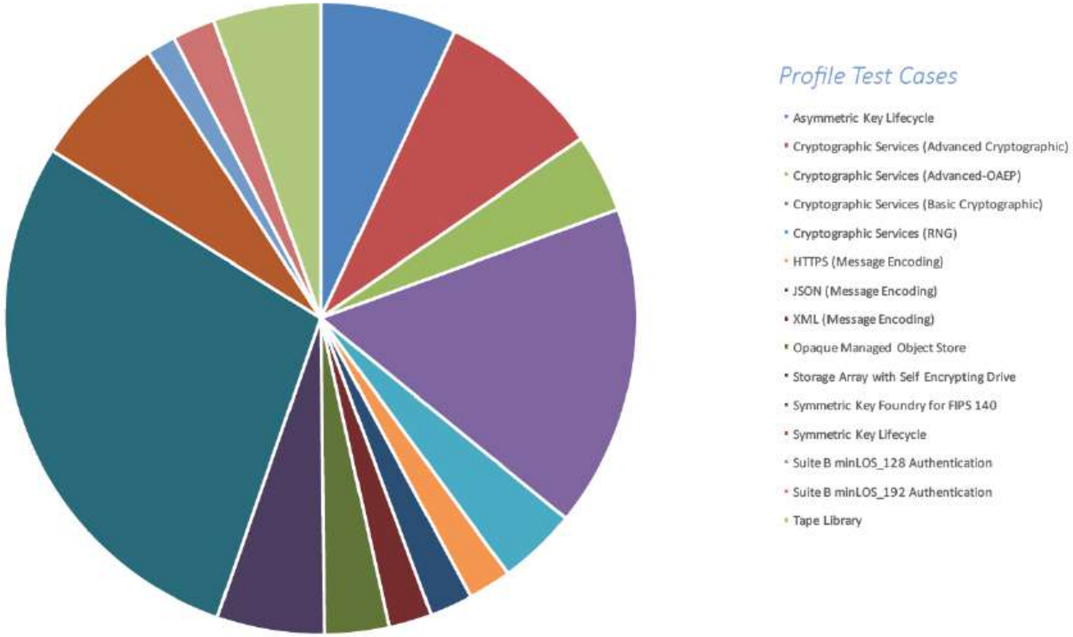
- Profiles outline a mandatory (with some allowed variation) set of conformance requirements.
- Requirements are usually a subset of specific operations, attributes and other items combined with one or more request/response traces.
- Over 100 discrete profiles for clients and servers including:
  - Tape Library
  - Storage Array with SED
  - Suite B
  - Cryptographic Services
  - Opaque Managed Object Store
- A range of new profiles under construction

KMIP Profiles



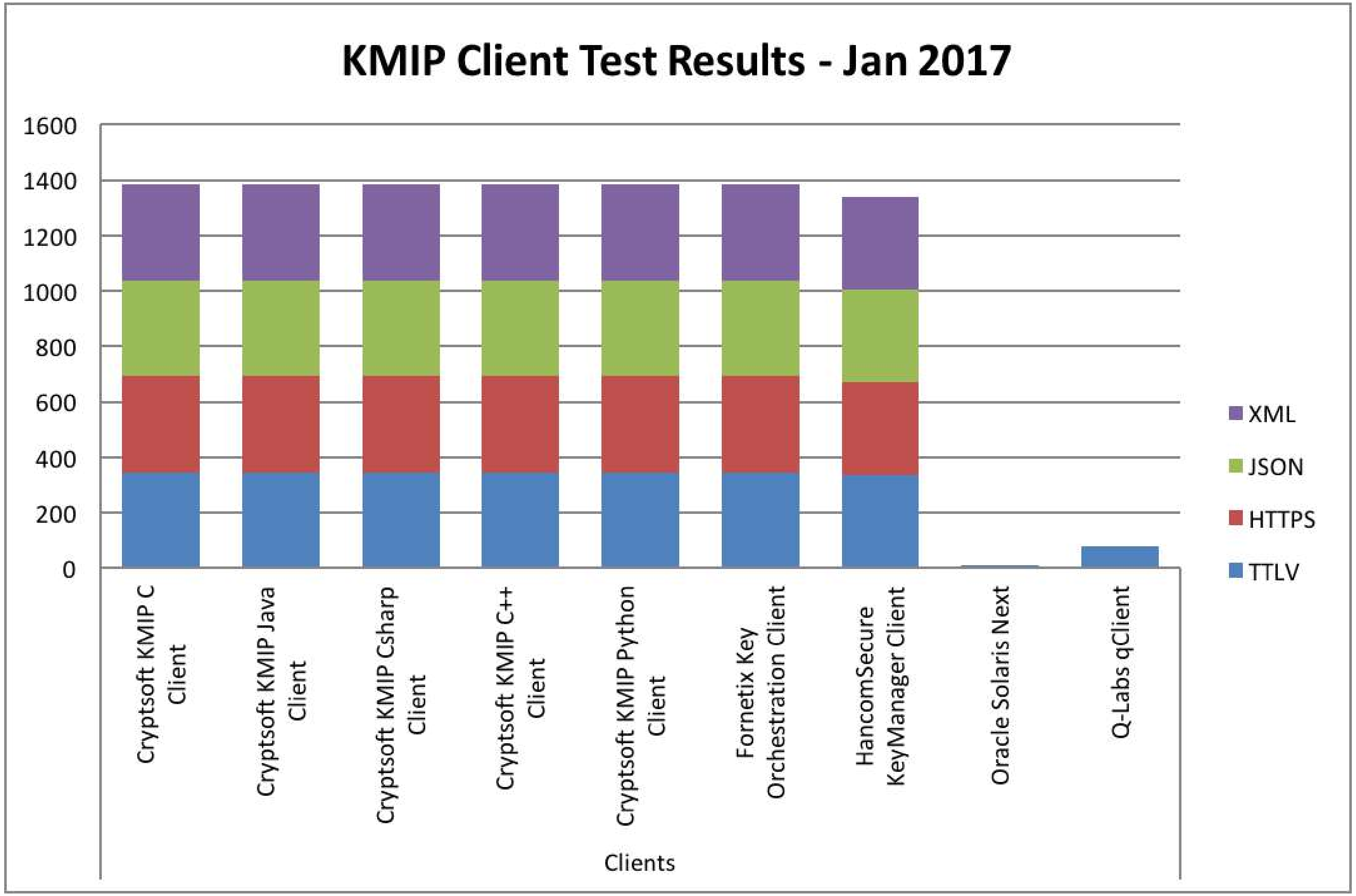






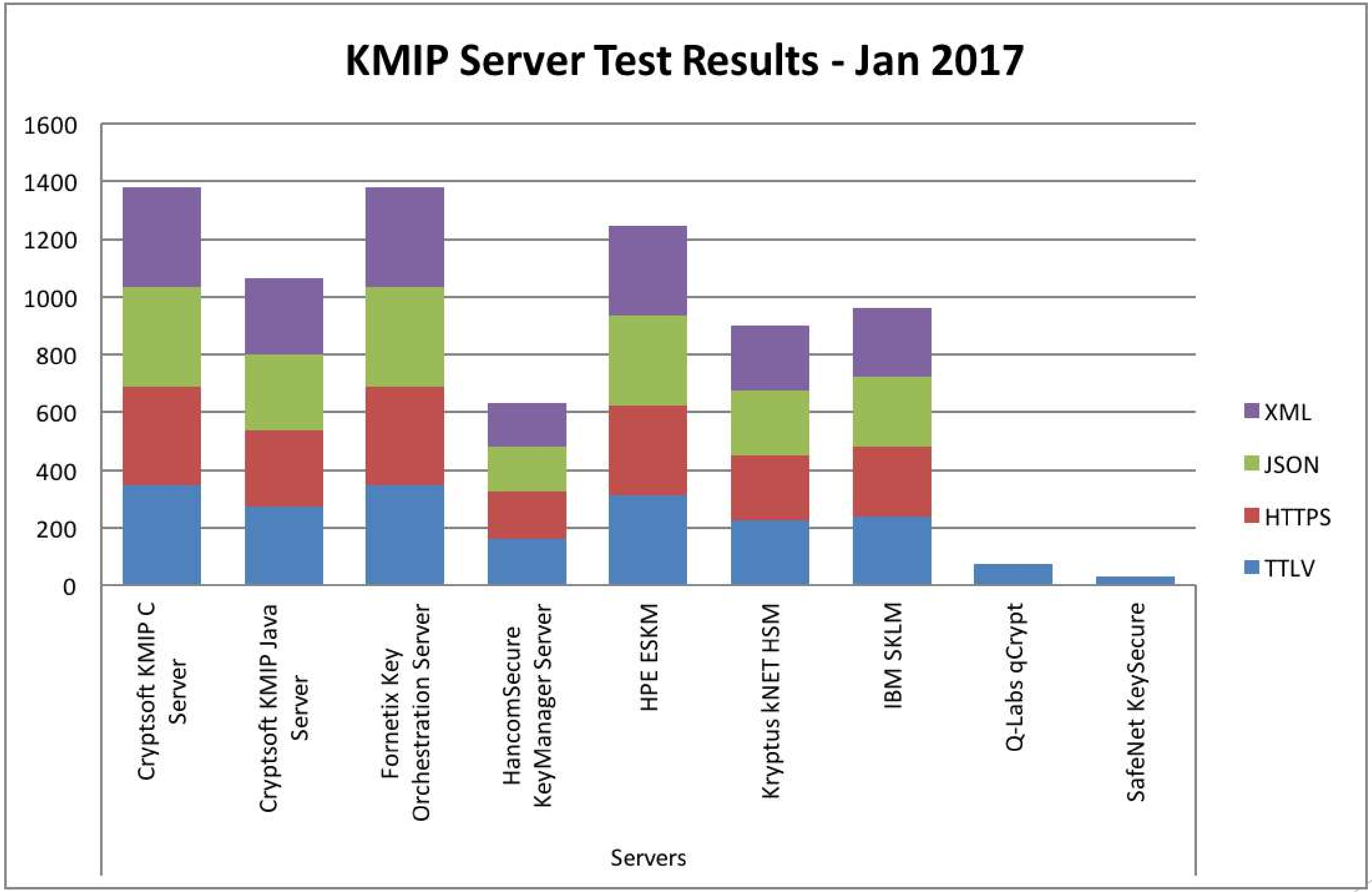
* Source: Cryptsoft

KMIP Interoperability – Client testing



* Source: Cryptsoft

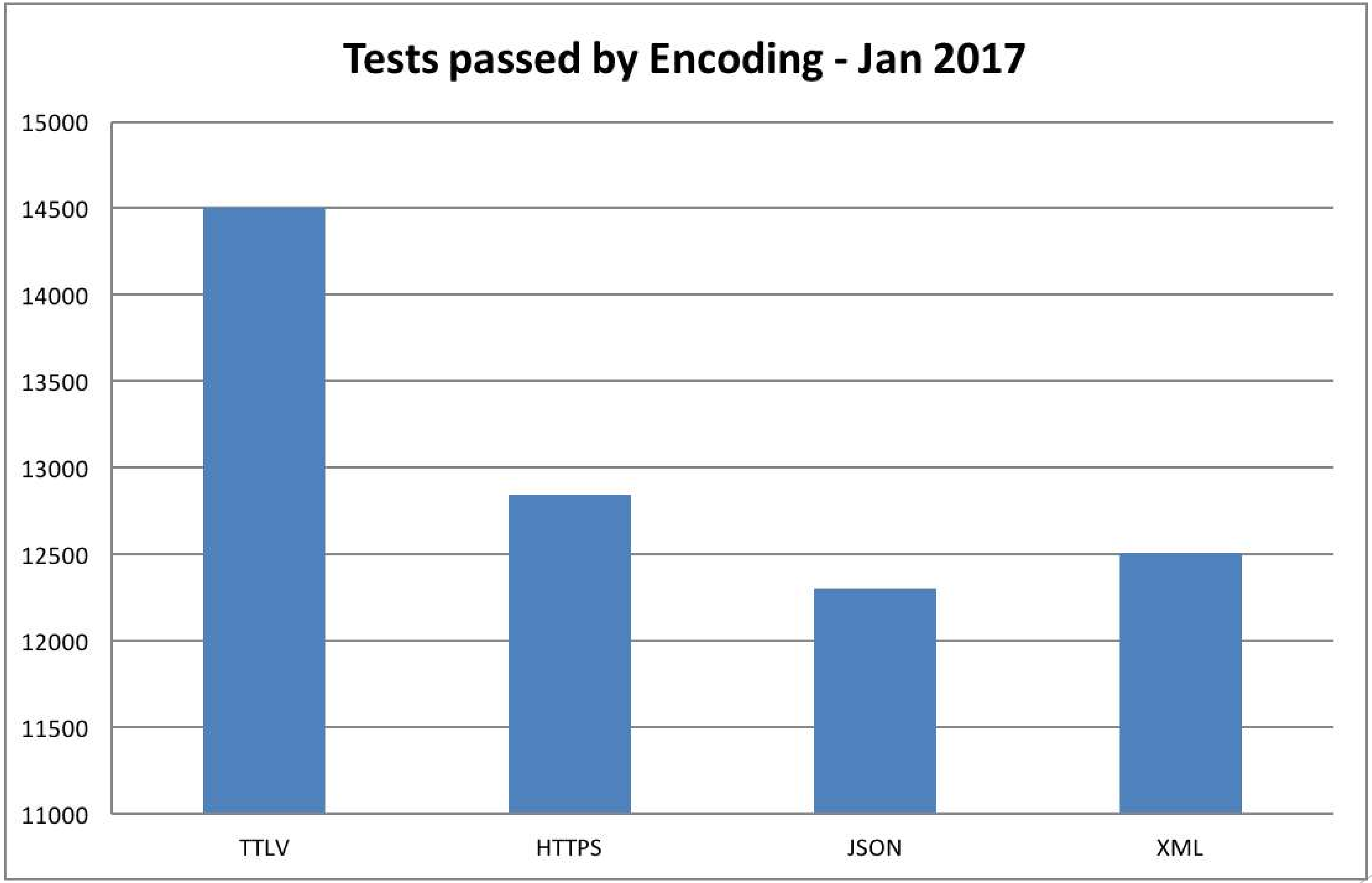
KMIP Interoperability – Server testing



CRYPTSOFT

* Source: Cryptsoft

KMIP Interoperability Testing



* Source: Cryptsoft

KMIP - Where to from here?

- KMIP Technical Committee is focused on KMIP v2.0 with particular attention to:
  - PQC response to ensure ongoing, interoperable security
  - Greater volume of industry-specific profiles
  - Streamlined, secure deployment and registration of KMIP clients:
    - Cloud context
    - Critical Infrastructure context

KMIP & Smart Grid

Smart Grid KMIP Deployment

- Key management platform for DLMS/COSEM
- Multiple server vendors gearing to support implementations
  - Common requirement for FIPS 140-2, level 3
- Multiple procurement events underway in Europe
- Interest from the US Smart Grid market
- Main focus on support for Symmetric keys, with some certificates and asymmetric key pairs also in use
- Work ongoing for managing authentication credentials

Summary – KMIP Benefits for Smart Grid

- An active Cybersecurity community developing security products to meet current and future needs for Smart Grid and IOT.
- Reduced investment in developing and researching complex, fixed, key hierarchy models
- Increased redundancy through use of common infrastructure using off-the-shelf products
- Greater ROI through re-use of existing integrations and greater competition between vendors
- Increased levels of security as the same vendors are working to meeting increasing data & privacy requirements.

Further work with the KMIP TC

- Requirements are always welcome:
  - Join OASIS and contribute directly
  - Pass requirements through existing relationships with existing members
  - Contribute via email (see https://www.oasis-open.org/committees/comments/index.php?wg_abbrev=kmip)
- Other Technical Committees focused on other areas of Smart Cities & Smart Grids (see https://www.oasis-open.org/

CRYPTSOFT

Questions?

Thank You!

tony.cox@cryptsoft.com

CRYPTSOFT