RSA Conference 2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: PDAC-F03

Encryption without key management – It's like Icing without the cake

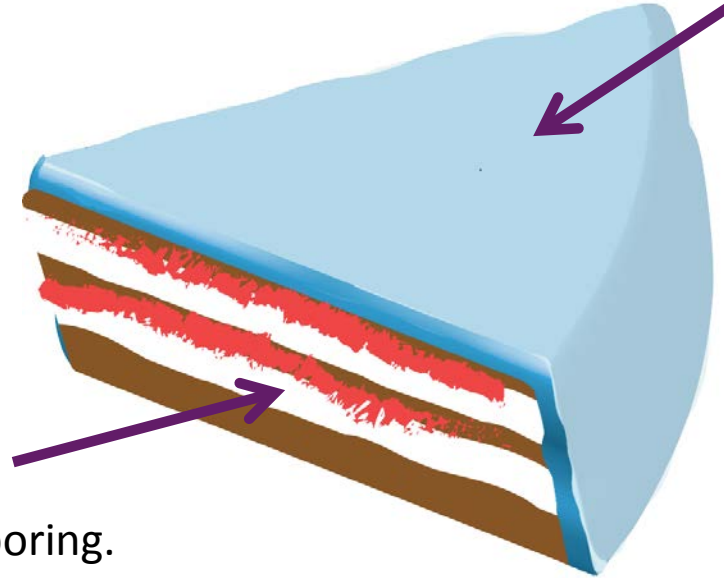
Saikat Saha
Sr. Principal Product Manager
Database Security
Oracle Corporation

Tony Cox
Director, Strategy & Alliances
Cryptsoft

Icing Without The Cake

Encryption and related security technologies

Highly important, mandated and exciting!

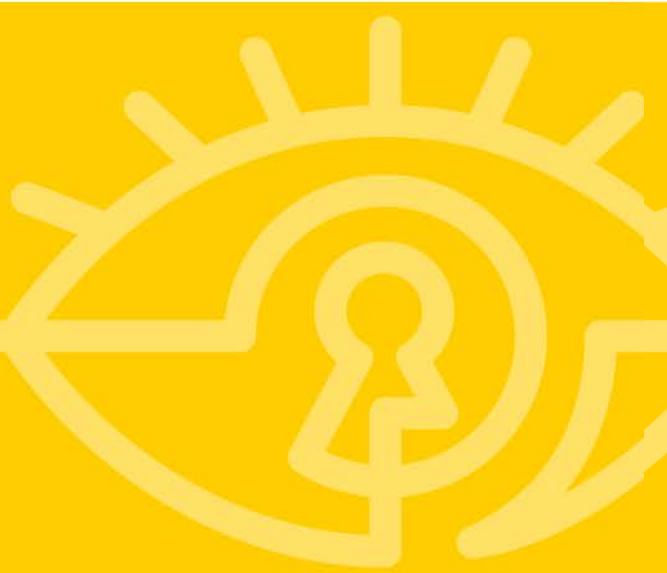


Key Management

Absolutely critical, but boring.

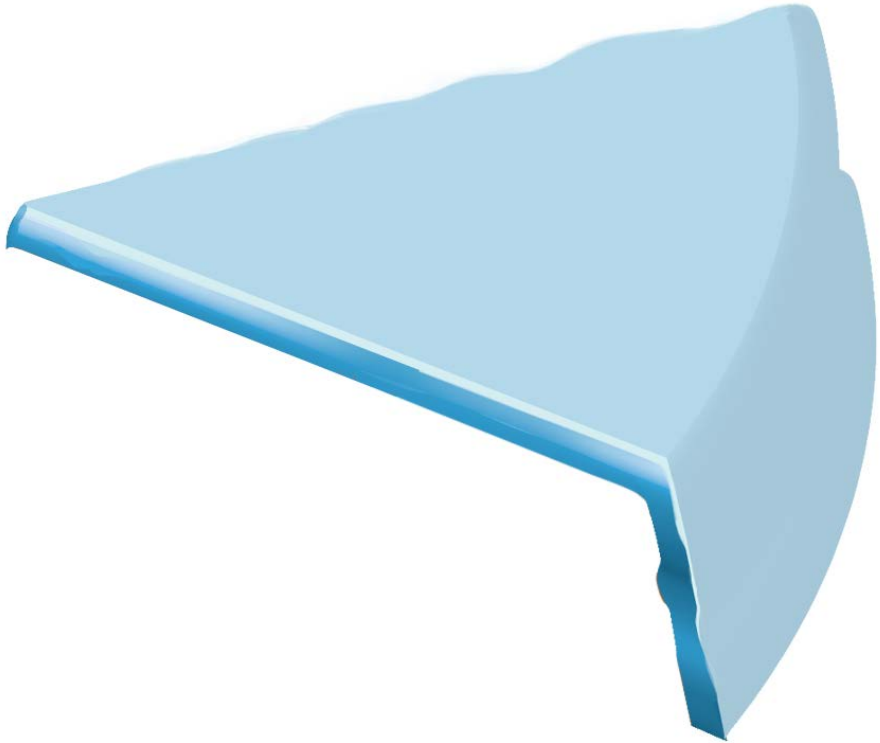
Agenda

- Encryption - Core to Data Security
- Key Management Challenges and Regulations
- What is Key Management?
- KMIP Fundamental and Evolution (1.0, 1.1 & 1.2)
- KMIP Implementation and Interoperability
- KMIP Future (1.3, 1.4 & beyond)
- How to “Apply”?



Encryption - Core to Data Security

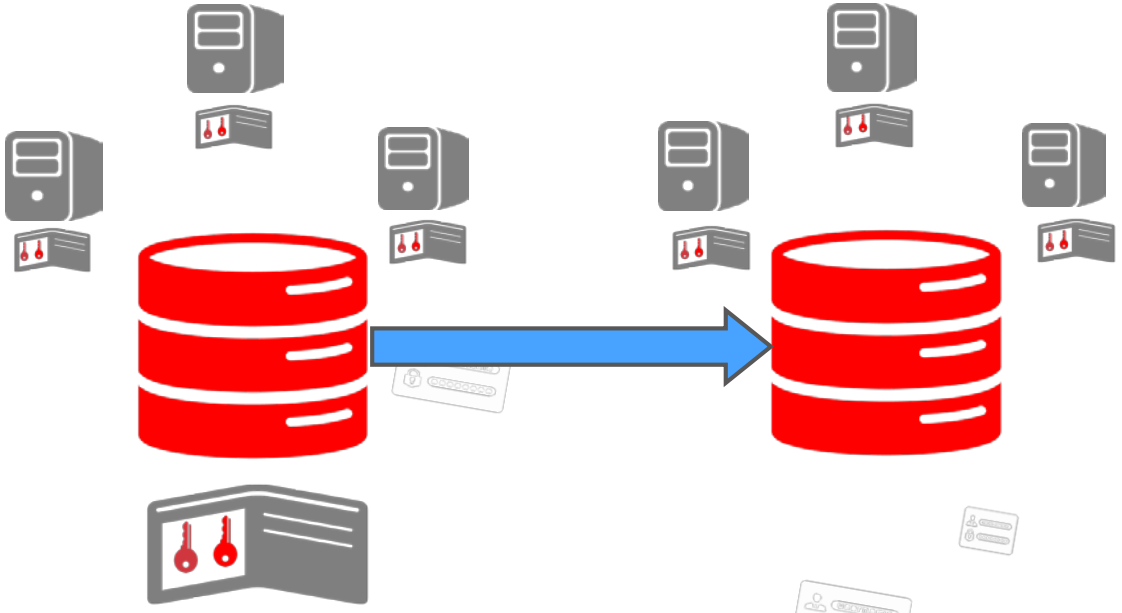
Encryption – the icing



Encryption is Everywhere

- Encryption is critical to data security
  - Data-at-rest
  - Data-in-transit
- Data-at-rest Encryption
  - Application encryption
  - Database encryption
  - File encryption
  - Disk/Storage encryption
- Encryption is mainstream now!

Management Challenges: Proliferation

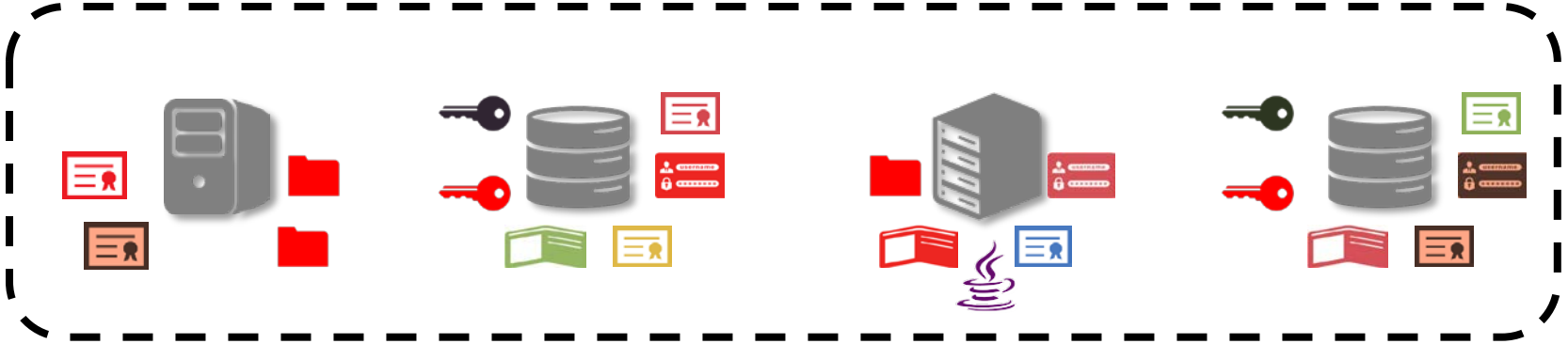


Primary Data Center

Failover Data Center

Key Management Challenges and Regulations

The Challenges of Key Management



Management

- Proliferation of encryption wallets and keys
- Authorized sharing of keys
- Key availability, retention, and recovery
- Custody of keys and key storage files

Regulations

- Physical separation of keys from encrypted data
- Periodic key rotations
- Monitoring and auditing of keys
- Long-term retention of keys and encrypted data

Regulatory Drivers

PCI DSS v3.1
April 2015

PCI Security Standards Council

3.5 Store cryptographic keys in a secure form (3.5.2), in the fewest possible locations (3.5.3) and with access restricted to the fewest possible custodians (3.5.1)

3.6 Verify that key-management procedures are implemented for periodic key changes (3.6.4)

And more!

Regulatory Drivers *contd…*

HIPAA – The US Health Insurance Portability and Accountability act (HIPAA) of 1996
HITECH – Health Information Technology for Economic and Clinical Health (HITECH) act

---

164.312 (a)(2)(iv) 164.312 (e)(2)(ii) 164.312(e)(2)(i) 164.312(c)(2)
Encryption and Decryption, Integrity, Mechanism to Authenticate electronic health information

164.312 (a)(2)(iv) 164.312 (e)(2)(i)
Encryption and Decryption, Integrity Controls
Effective Key management and protection must be demonstrated to support the encrypted state of data

Regulatory Drivers *contd…*

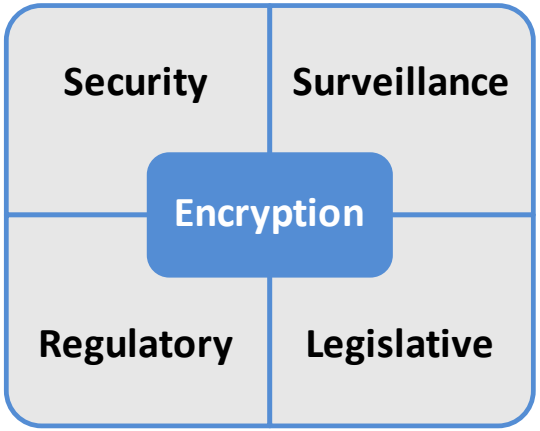
GDPR : Global Data Protection Regulation
EEA : European Economic Area Controller

ARTICLE 30: ENCRYPTION AND PSEUDONYMISATION
The controller and the processor ... as appropriate: the pseudonymisation and encryption of personal data

ARTICLE 28: Each controller and, if any, the controller's representative, shall maintain a record of processing activities under its responsibility

EEA 54a: Methods to restrict processing of personal data could include ... making the selected data unavailable to users or temporarily removing published data from a website

Encryption is the easy part



Key Points

- Encryption is easy, fast, ubiquitous
- Encryption is inexpensive

Deploying encryption solutions is easy

- **Encryption is now ubiquitous**
- **Encryption is in software**
- **Encryption is in hardware**
- **Encryption libraries are easily supported**
- **Encryption is cheap and easy to use**
- **Encryption is fast** (AES-NI, line rate, encrypting HBAs, et.al)

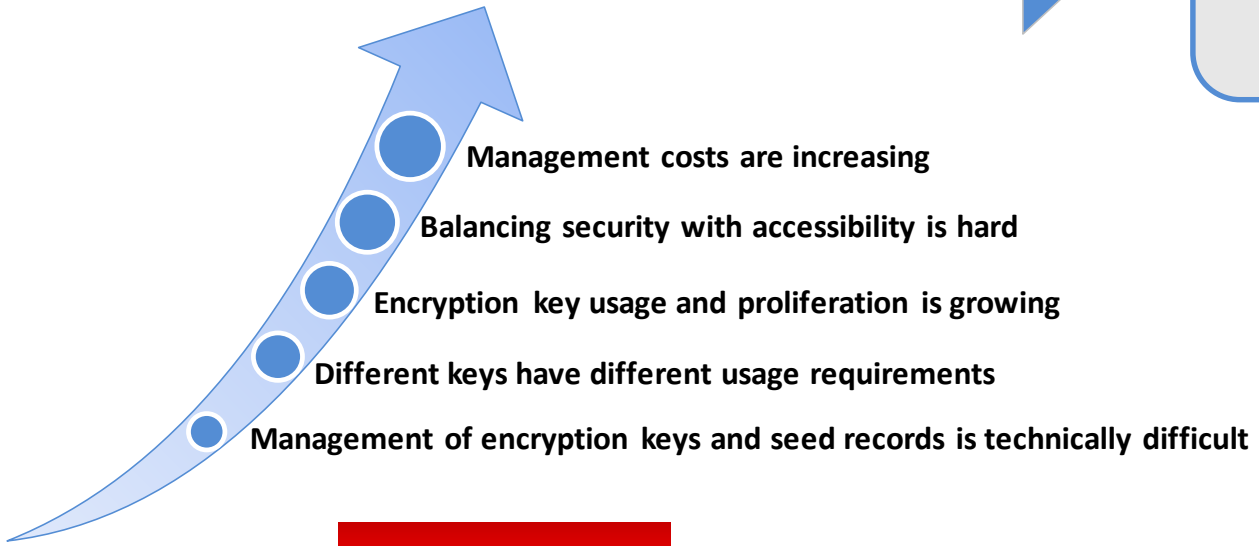
Key management is hard

Key Points

- Key loss results in data loss
- Key compromise results in data compromise

Key management is critically important

Key Management Problem



KMIP is the solution

What is the solution?

KMIP
KEY MANAGEMENT INTEROPERABILITY PROTOCOL

Key Point

- KMIP is the solution to your key management problem

- *Leave it to specialist security vendors*
- *Use independent conformance testing programs*
- *Avoid platform and technology lock-in*
- *Externalise the problem from your domain*
- *Use open vendor neutral standards*
- *Avoids vendor lock-in*

Designed by the industry's most experienced vendors

Active on-going standards development / evolution

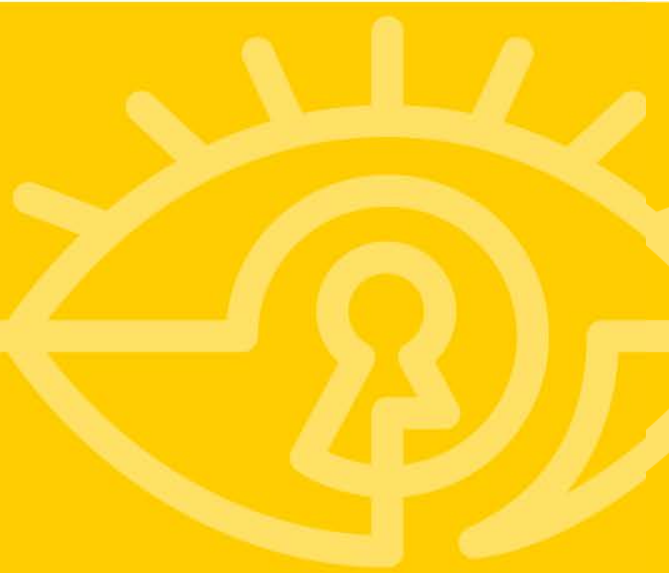
Deployed in wide range of products from multiple vendors

Successful transition from standard into products

Open standard under open management (OASIS)

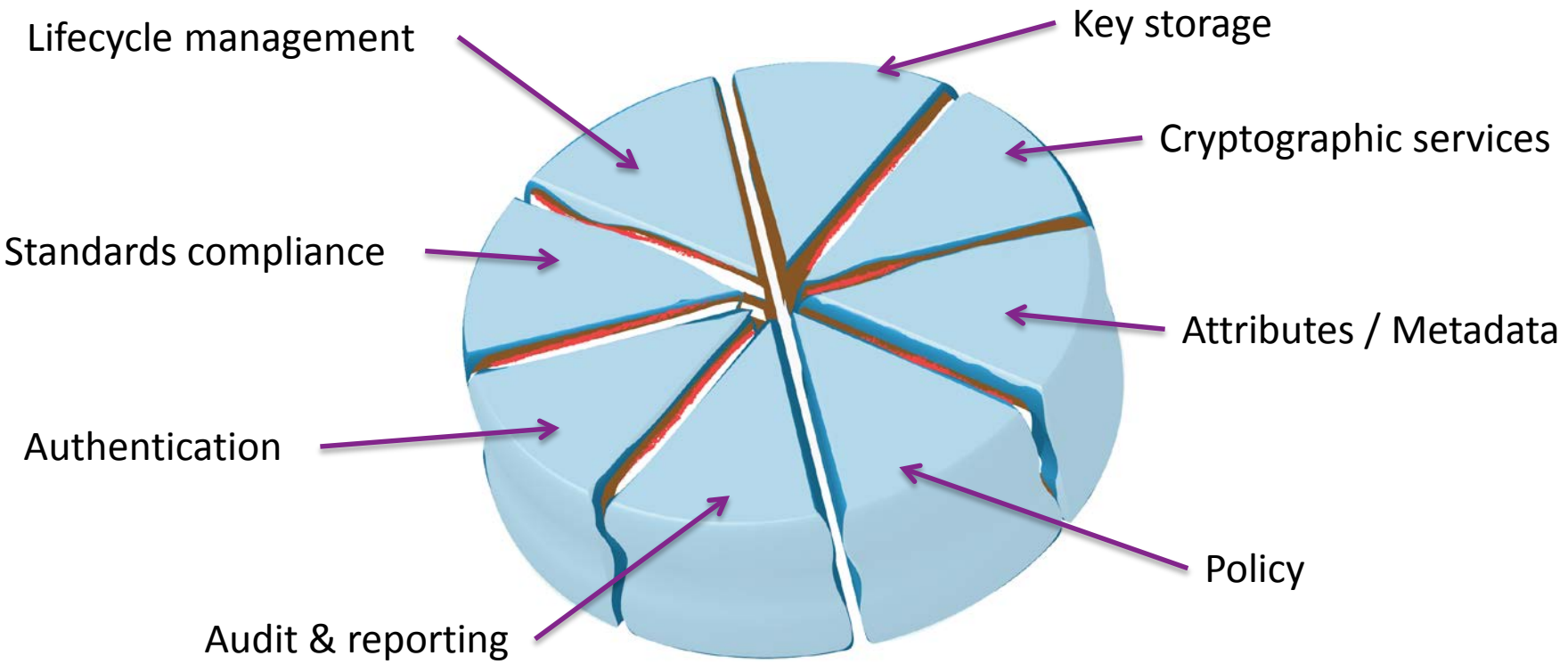
Multiple independent interoperable implementations

OASIS
CRYPTSOFT
ORACLE



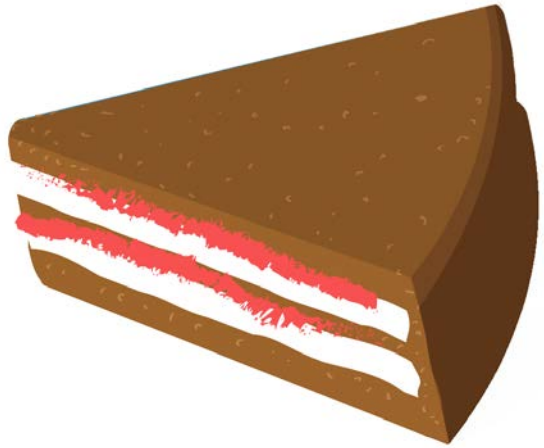
What is Key Management?

Key Management - the cake



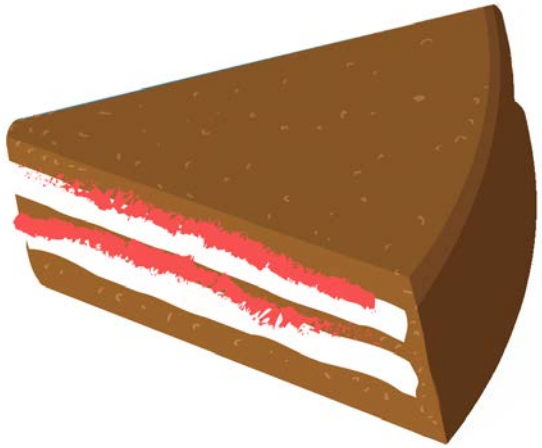
What is Key Management?

- Lifecycle management
  - Minimum operation set – Create, Register, Destroy, Rekey
  - KMIP has a very rich set of operations (40+ operations)
  - KMIP Specifies NIST 800-57 states and transitions



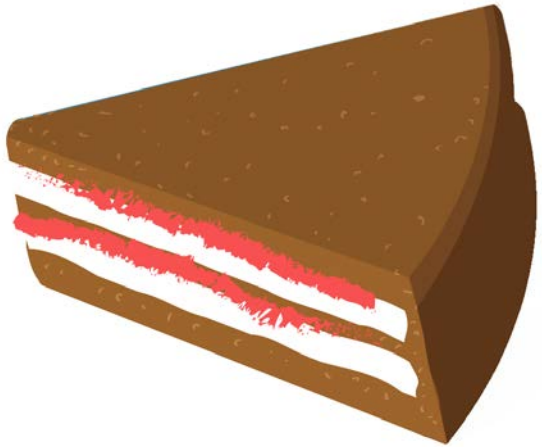
What is Key Management?

- Key storage
  - Simple flat file
  - Detailed register
  - Secured (kek or keystore encryption)
  - Offload (HSM/EKM)



What is Key Management?

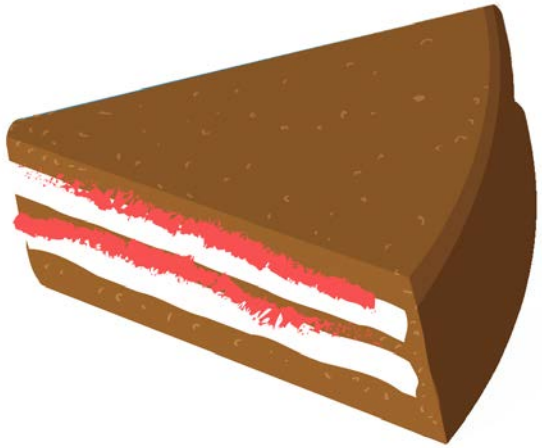
- Attributes / Metadata
  - KMIP allows for an almost unlimited number of attributes per key (object)
  - Multiple attribute types
  - Custom attribute types (usually best avoided)



What is Key Management?

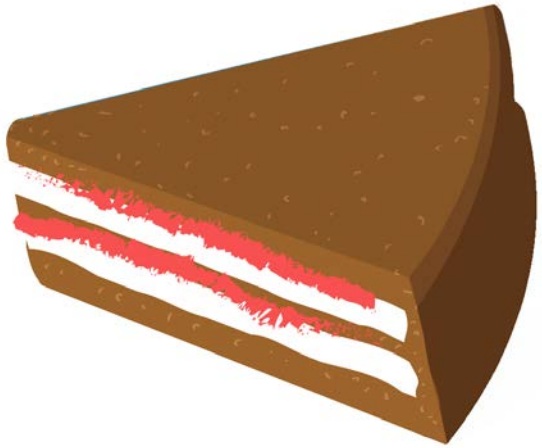
- Authentication
  - User access
  - Device access
  - Admin access

KMIP Clients



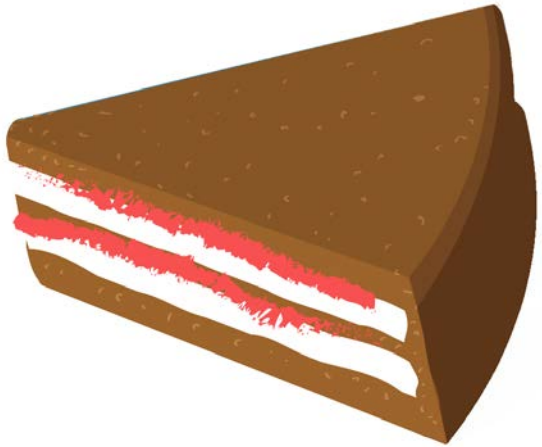
What is Key Management?

- Cryptographic Services
  - Provide a richer set of functionality
  - KMIP operations include:
    - Encrypt & Decrypt
    - Sign & Verify
    - Hash, MAC & MAC verify
  - Supplement or replace HSMs



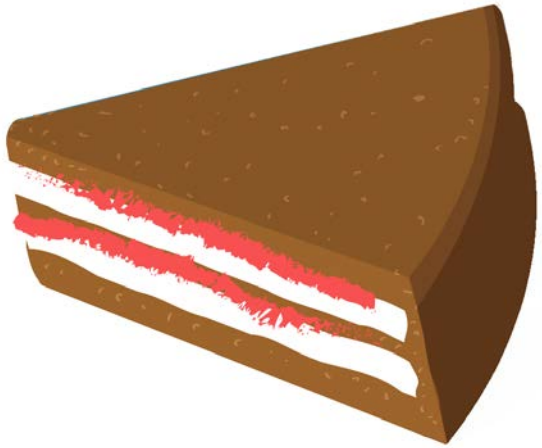
What is Key Management?

- Audit & Reporting
  - Used to answer a range of questions:
    - How many keys?
    - Of what type?
    - Used for what?
    - Used how often?
    - Used by who/what?
  - Forms the basis of compliance reporting



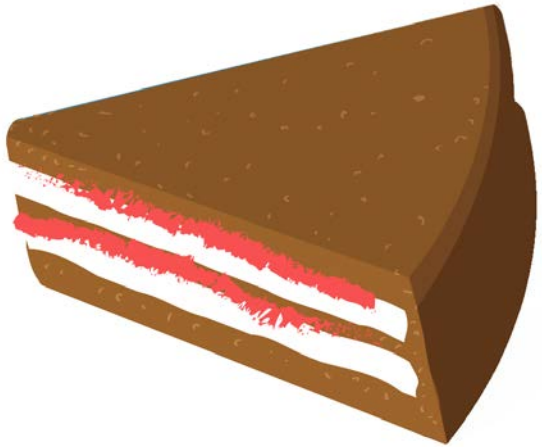
What is Key Management?

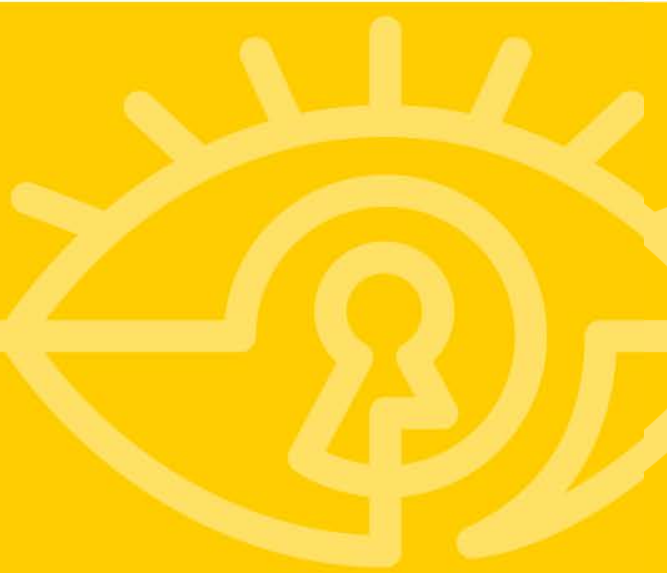
- Policy
  - Authorisation
  - Scheduling
  - Compliance enforcement



What is Key Management?

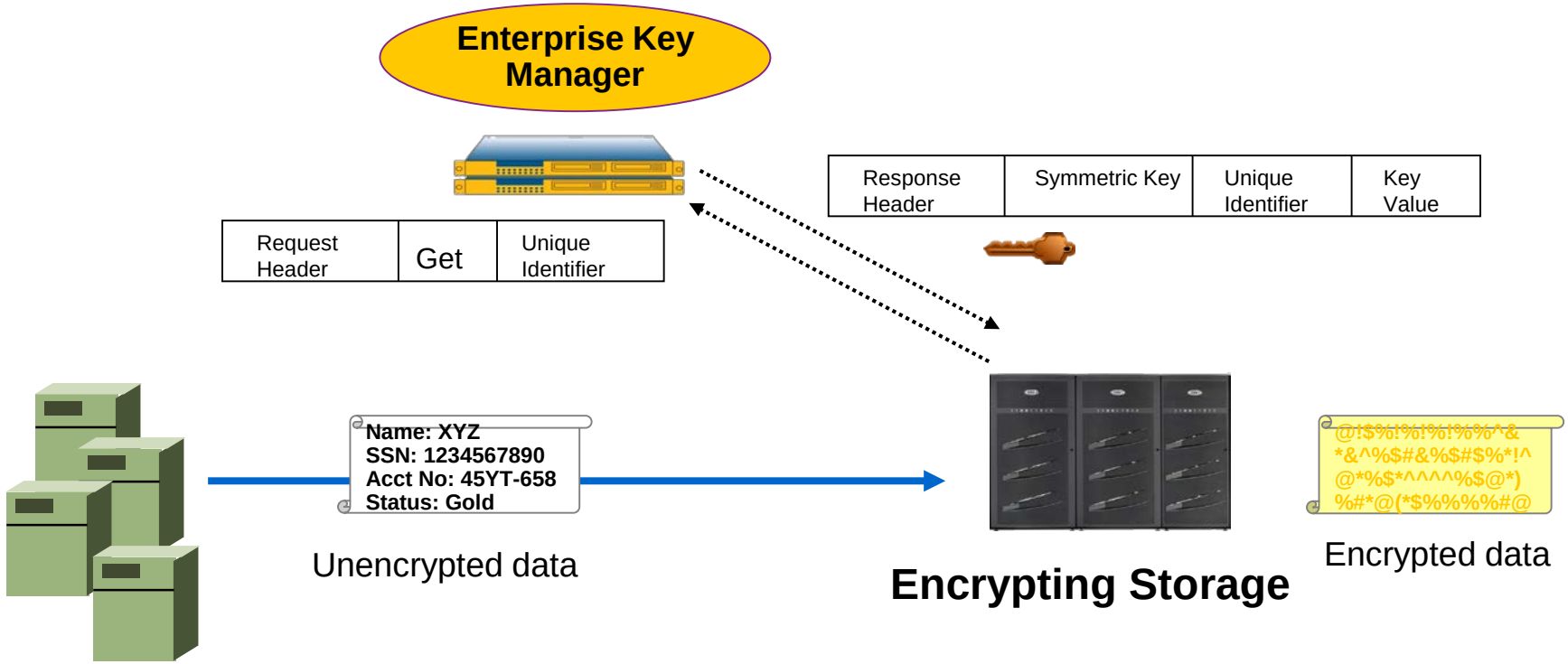
- Standards compliance
  - Minimum standards (NIST etc)
  - Ideal = KMIP
    - Open standard under open management (OASIS)
    - Active standards development / evolution
    - Designed by the industry's most experienced vend
    - Deployed in wide range of products from multiple vendors





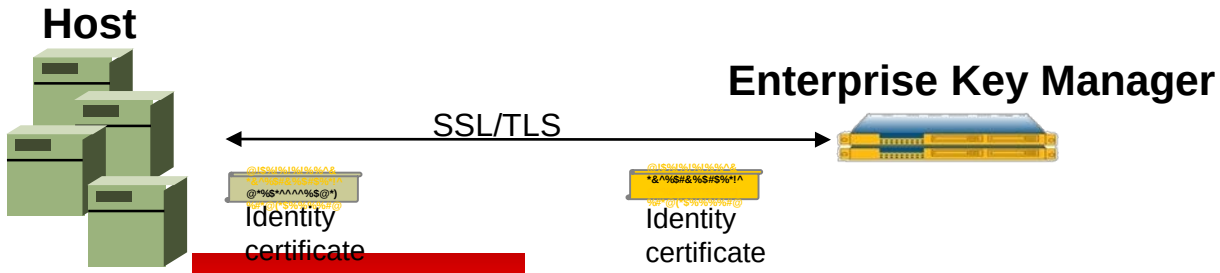
KMIP Background and Evolution

KMIP Request / Response Model

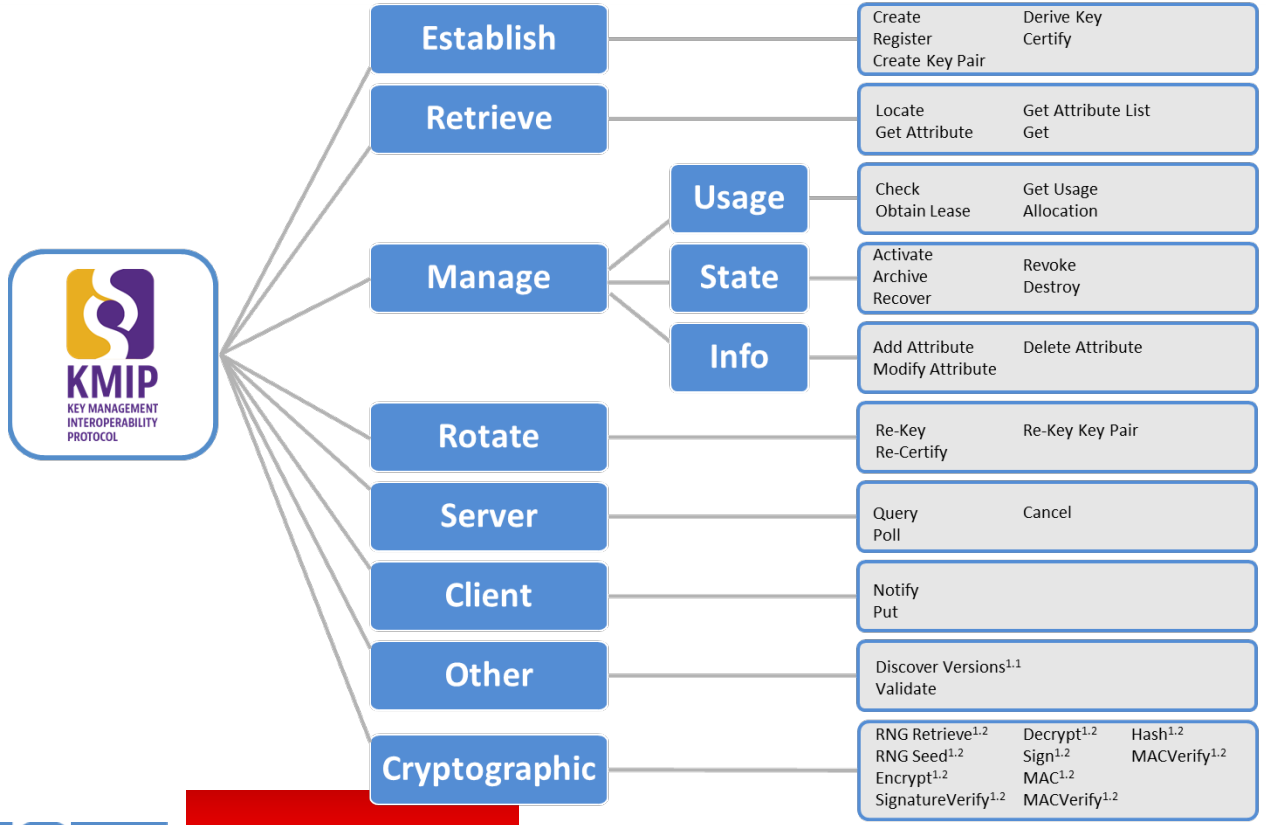


Authentication

- Authentication is external to the protocol
- All servers should support at least
  - TLS V1.0
- Authentication message field contains the Credential Base Object
  - Client or server certificate in the case of TLS

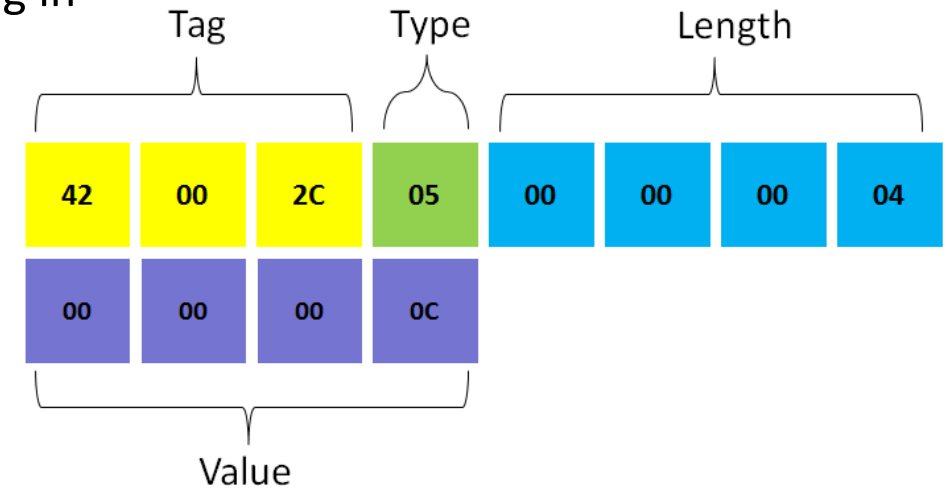


KMIP Fundamentals



KMIP Fundamentals

- Message Encoding
  - Binary Tag-Type-Length-Value format
  - Optional JSON and XML encoding in KMIP[1.2]

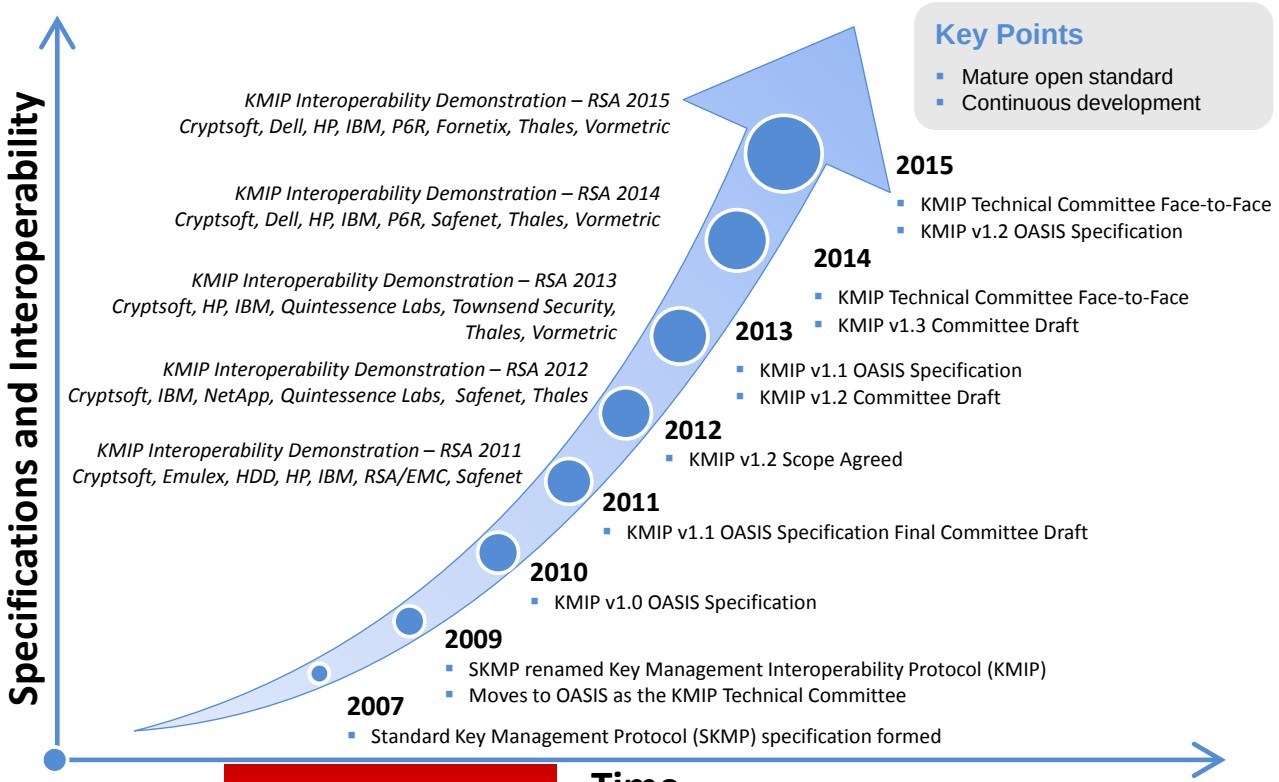


Cryptographic Usage Mask = Encrypt | Decrypt

KMIP Specification Development

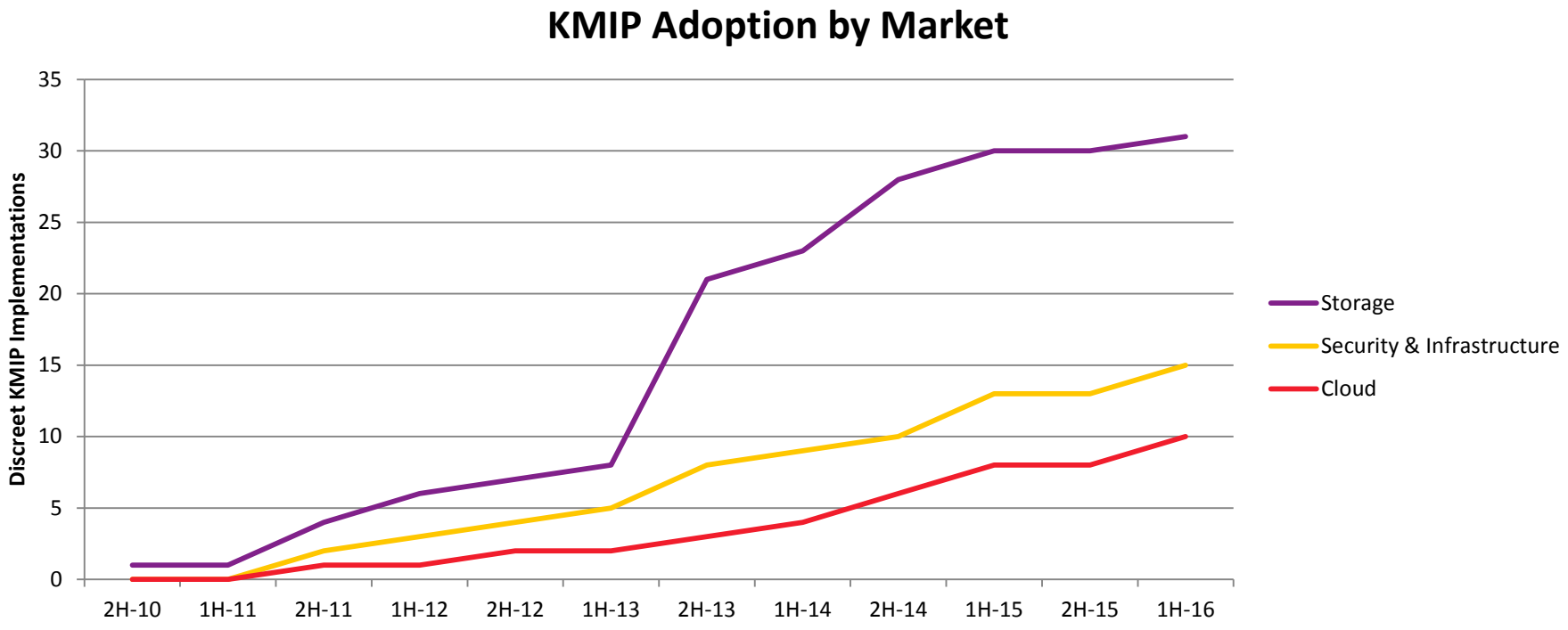
- OASIS KMIP 1.0 – Oct 2010
  - Full NIST life-cycle support
  - Symmetric, PublicKey, PrivateKey, Certificate, SecretData, SplitKey, Opaque
  - Small set of profiles
- OASIS KMIP 1.1 – Jan 2013
  - DiscoverVersions, ReKeyKeyPair
  - Fresh and Object Group Member
  - QueryExtensionList, QueryExtensionMap
- OASIS KMIP 1.2 – May 2015
  - PGP Key Object Type
  - Alternative Name
  - Cryptographic Services
  - Attestation
  - Create/Join SplitKeys
  - External Key Handling (MDO)
  - HTTPS transport
  - JSON and XML encoding
  - Profiles with test cases

KMIP Progression



KMIP Implementation and Interoperability

KMIP Market Adoption



KMIP Deployments

Storage

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

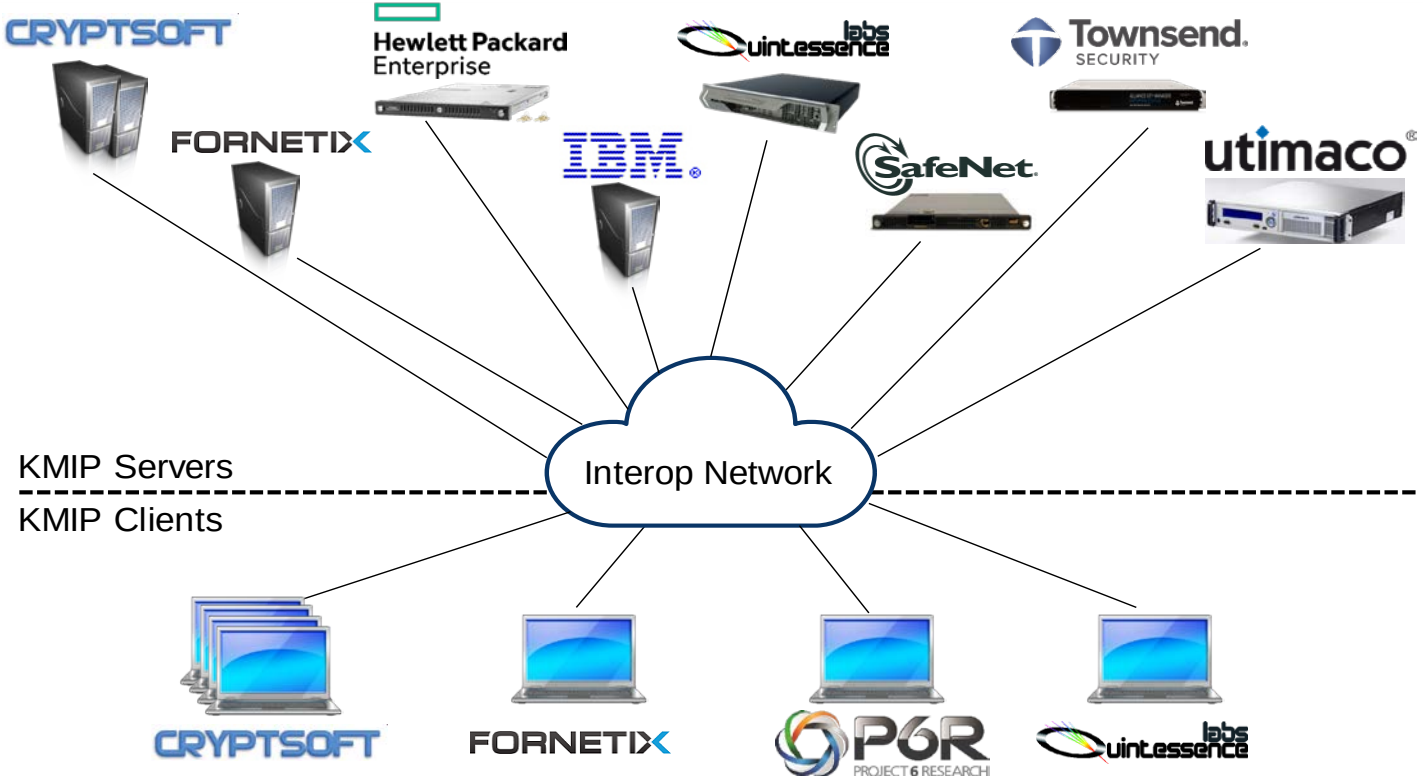
Infrastructure and Security

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

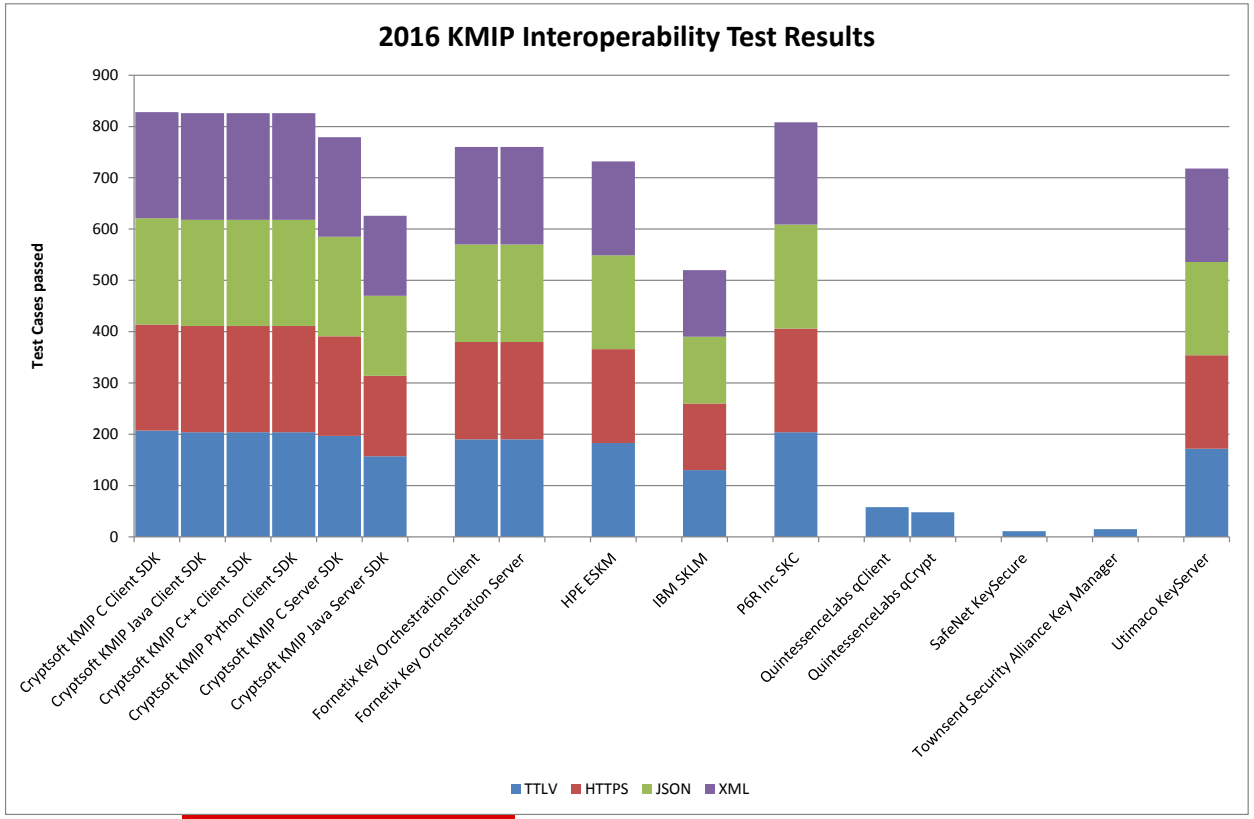
Cloud

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

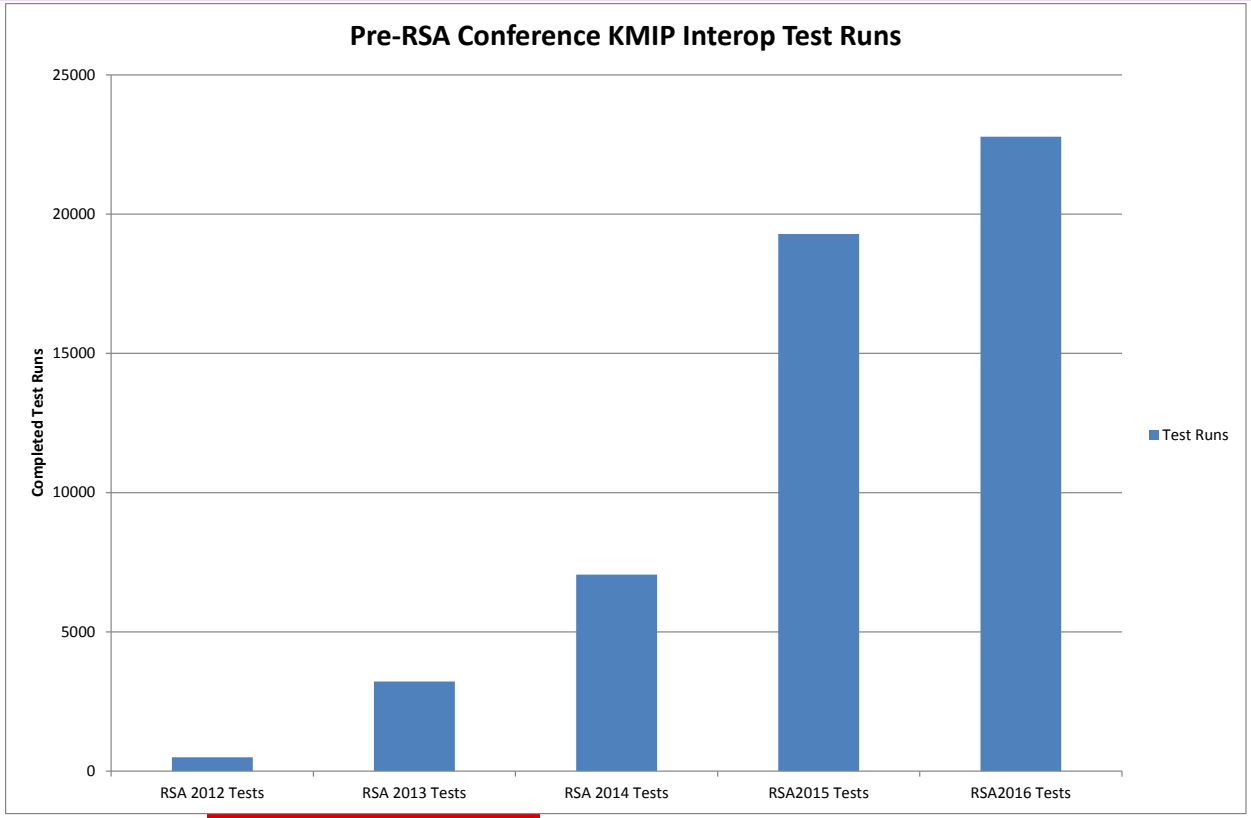
KMIP Interop Testing



KMIP Interop Testing 2016

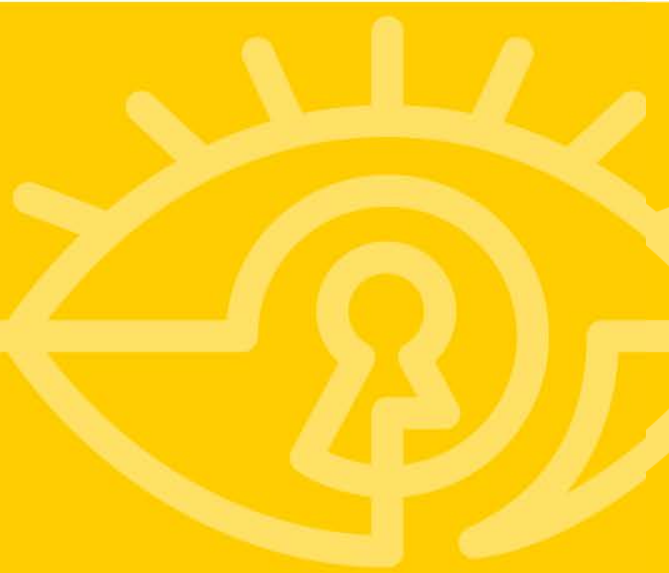


KMIP Interop Testing



KMIP Conformance

- KMIP Conformance Testing program
  - Run by Storage Networking Industry Association (SNIA) within the Storage Security Industry Forum (SSIF) - http://www.snia.org/forums/ssif/kmip
  - Program is gaining momentum with tests completed by:
    - Cryptsoft (1 Server SDK, 1 Client SDK)
    - HPE (1 Server, 1 tape library)
    - IBM (1 server)
    - More in the queue….



KMIP Future

KMIP 1.3

- Adjustments to improve interoperability
- Deprecated Template Managed Object
- Deprecated Default Operation Policy
- Generic Transparent EC Key Types
- Query RNG/DRBG information
- RNG Attribute
- Query options for validation information (FIPS140,CC)
- Query options for profiles supported
- Cryptographic Services streaming support
- One-time Pad
- Locate Offset+Limit
- Automated client registration

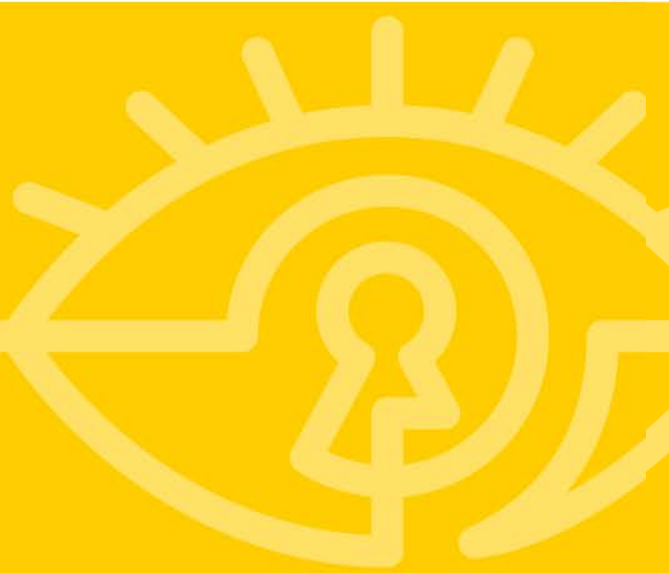
KMIP 1.4

Accepted

- PKCS#12 key format export option
- Query option for Server Batch Handling
  - Batch Undo
  - Batch Continue

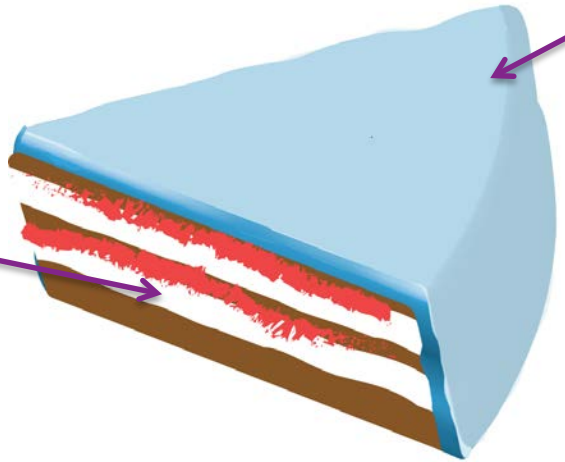
Under discussion

- PKCS#12 import
- General import/export
- Error handling
- Certificate Attributes
- Multiple CAs
- Request/Response Correlation
- Sensitive Attribute Handling



How to “Apply”?

Encryption and Key Management - Summary



Encryption and related security technologies

- Mandatory Requirement
- Exciting adjectives
- Many exciting form factors
- Well defined usage
- Solutions are widely available and varied
- Many solutions use proprietary key storage/management

Key Management

- Essential
- Boring
- Standardized
- Range of deployment options
- Well defined usage
- Widely supported industry standard