CRYPTSOFT

FOUNDATION SECURITY TECHNOLOGIES
TRUSTED^2| EMBEDDED| INTEROPERABLE

KEY MANAGEMENT: Truths and Consequences

01000011010100100101100101010000010101000101001101001111010001100

Date:07/2015

Abstract

KEY MANAGEMENT: Truths and Consequences

The imperative to encrypt data has driven the strong and sustained growth in the Enterprise Key Management market.

Gaining accurate knowledge and clear insight into this market is a significant challenge both for vendors and end-users. Publically accessible information is littered with half-truths, misdirection and creative marketing content. Failing to distil reality from fantasy will undermine your ability to make the critical decisions you need stay competitive.

This session will provide you with the inside information about what was, what is and what will be in the next 18 months of Enterprise Key Management."

Enterprise Key Management:

Truths: Where the encryption imperative came from

Human (ID10T) Errors

In **1990**, a laptop containing plans for the first Gulf War was stolen from the boot of a car in west London. The computer contained detailed information about how the military planned to remove Saddam Hussein's forces from Kuwait.

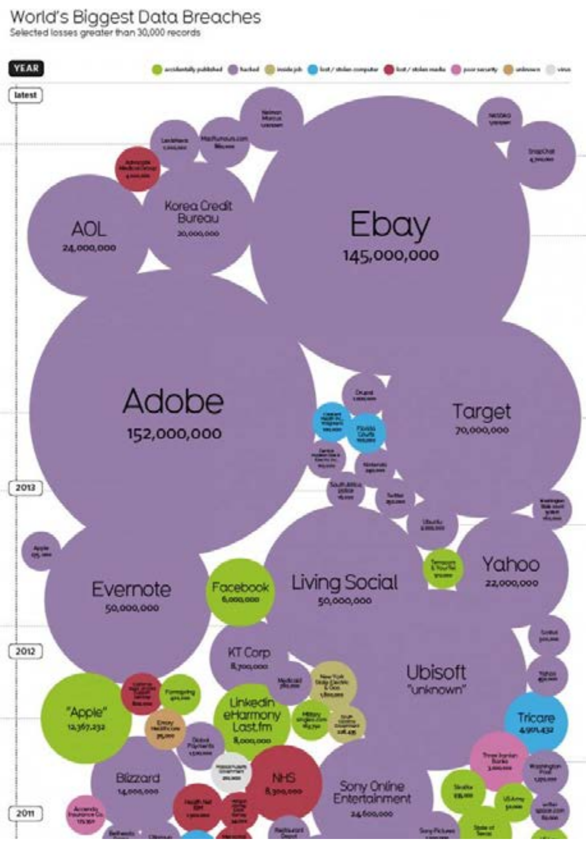
In March **2000** a laptop was stolen from the Kent home of John Spellar, who as Armed Forces minister was responsible for Britain's nuclear secrets and the military’s role in Northern Ireland.

In December **2007** – only months after the HMRC fiasco – it emerged that the names, addresses and phone numbers of 3 million driving test candidates were lost on a computer hard drive which went missing in the US.

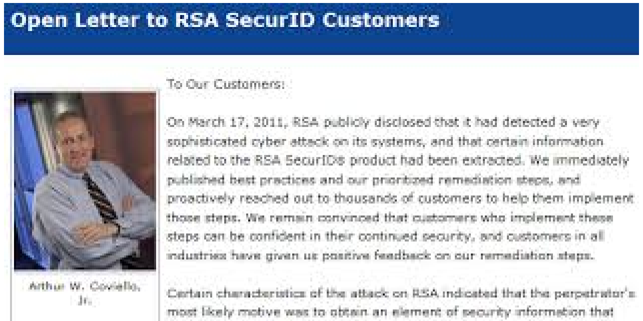
This week (**2011**), it was announced that GCHQ, the government eavesdropping centre, had tightened its security processes after losing hundreds of items of sensitive equipment worth £1million

© The Telegraph

Security Breaches



© databreaches.net



Open Letter to RSA SecurID Customers

Arthur W. Coviello, Jr.

To Our Customers:

On March 17, 2011, RSA publicly disclosed that it had detected a very sophisticated cyber attack on its systems, and that certain information related to the RSA SecurID® product had been extracted. We immediately published best practices and our prioritized remediation steps, and proactively reached out to thousands of customers to help them implement those steps. We remain convinced that customers who implement these steps can be confident in their continued security, and customers in all industries have given us positive feedback on our remediation steps.

Certain characteristics of the attack on RSA indicated that the perpetrator's most likely motive was to obtain an element of security information that

Surveillance

© Wired.com

Legislation

HIPAA Compliance

PCI Security Standards Council™

FSA Financial Services Authority

Sarbanes-Oxley

Solution

Encrypt Everything

Enterprise Key Management:

Truths: Opposing views

Opposing Views

Yes

- Enterprise Key Management is the solution

No

- Enterprise Key Management is not the solution

Opposing Views

Yes

- We have Enterprise Key Management and are committed to the solution
- We have a solution but we don’t want you to know about it

No

- Enterprise Key Management is not the solution
- We don’t really have a solution, but we’d like to pretend that we do

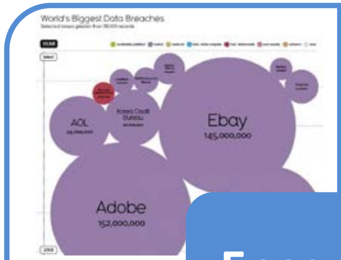
Cryptsoft as an Information Source

Enterprise Key Management:

Truths: Development of Enterprise Key Management

0100001101010010010110010101000001010100010100110100111010001100

Encryption is easy

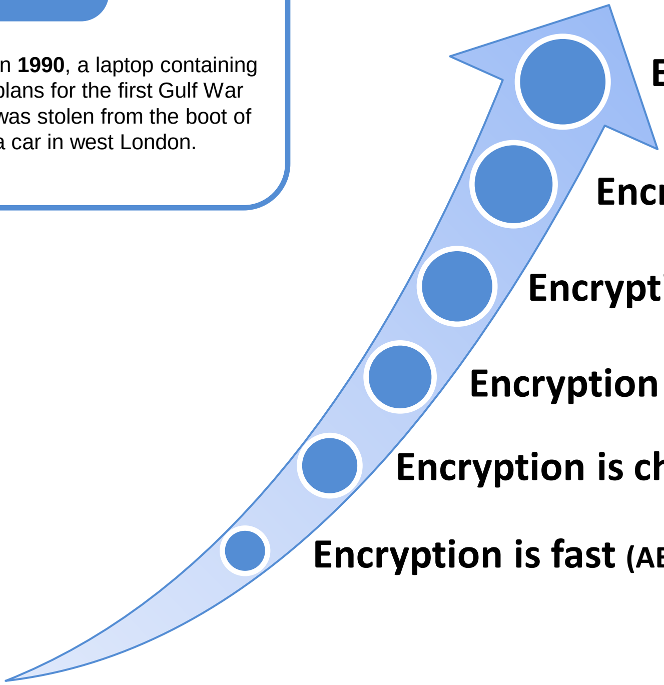


Encryption

HIPAA Compliance

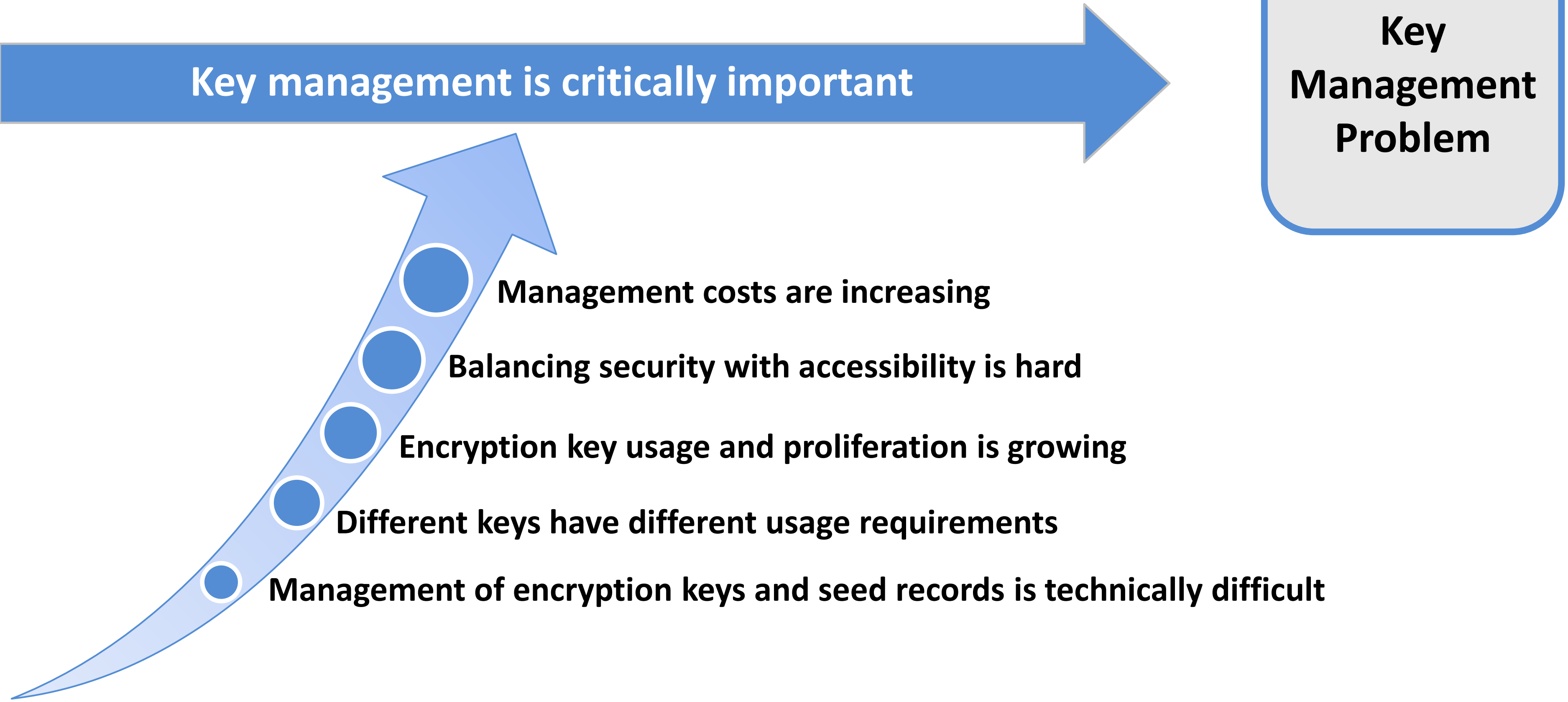
In **1990**, a laptop containing plans for the first Gulf War was stolen from the boot of a car in west London.

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 difficult



Key management is critically important

Key Management Problem

Management costs are increasing

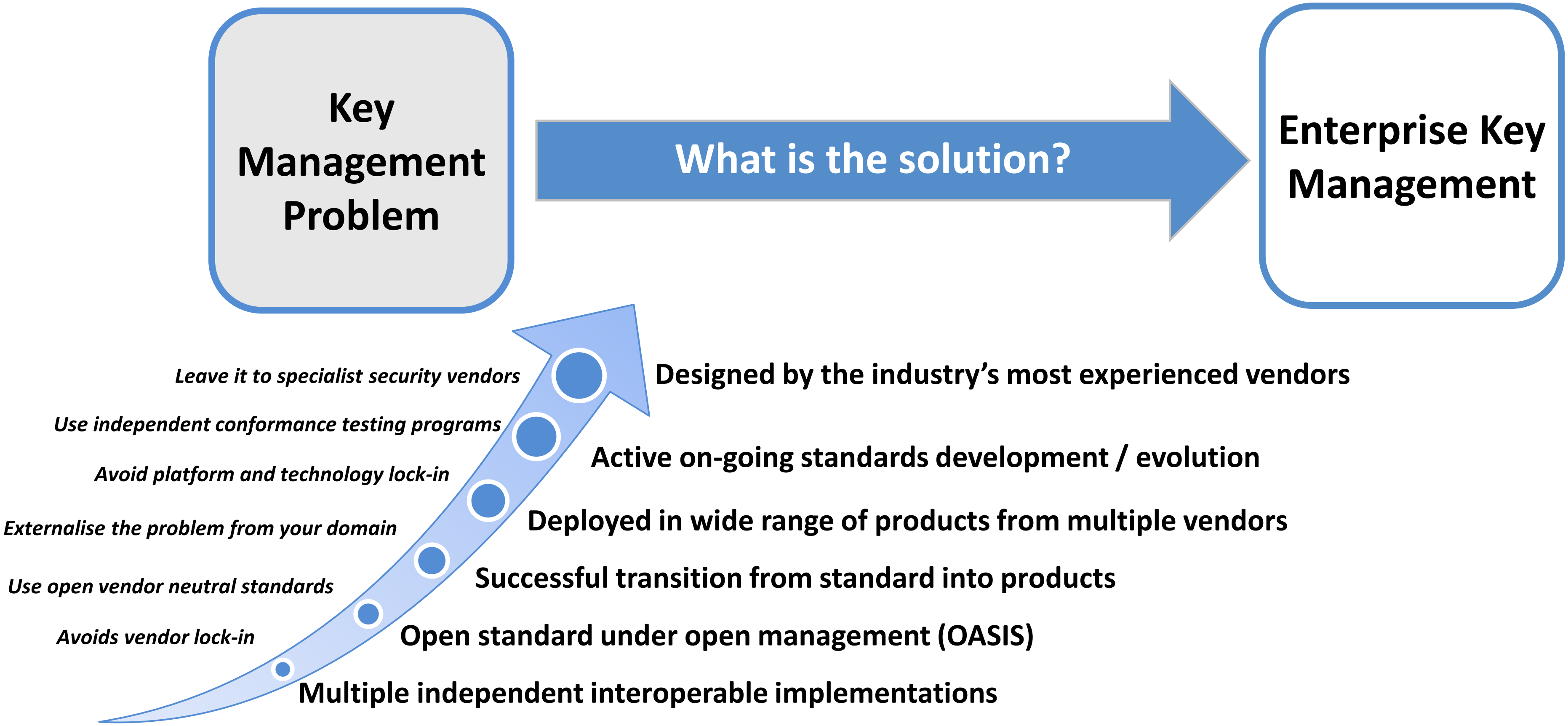
Balancing security with accessibility is hard

Encryption key usage and proliferation is growing

Different keys have different usage requirements

Management of encryption keys and seed records is technically difficult

Enterprise Key Management is the solution



Key Management Problem

What is the solution?

Enterprise Key Management

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

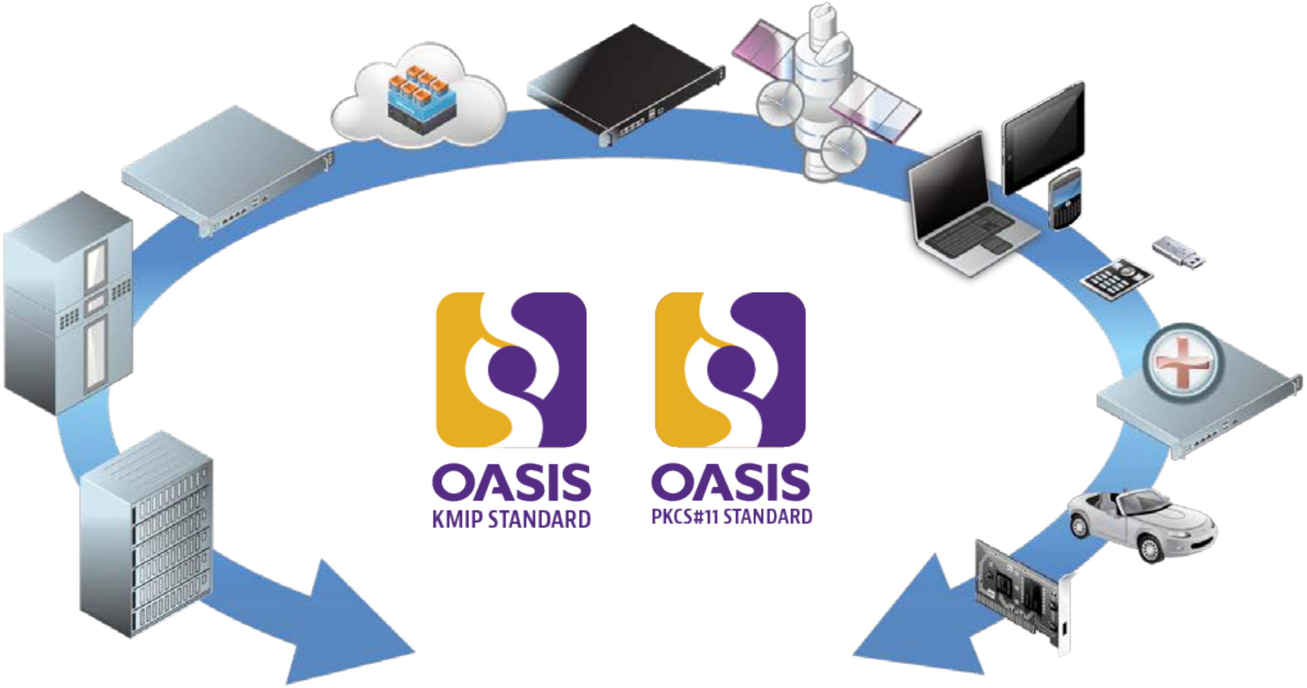
Enterprise Key Management:

Truths: Status of the current market - Who, What Where?

Where is enterprise key management used?

Enterprise Key Management

- Identification
- Mobile Devices
- Tape Libraries
- Disk Arrays
- Flash Arrays
- HSMs
- Virtual Devices
- Health Devices
- Satellite
- Automotive
- Embedded



Who has products in the market

BDT

DATASTAX

SEPATON

BROCADE

panzura

ETINET

NetApp

Hitachi Data Systems

Quantum

RSA
The Security Division of EMC

IBM

CRYPTSOFT

DELL
The power to do more

hp

CipherCloud
Trust in the Cloud™

THALES

SafeNet

Vormetric

BRACKET
COMPUTING

HUAWEI

ORACLE

EMC²

TREND
MICRO

FUJITSU

HYTRUST
Cloud Under Control

Townsend
SECURITY

VENAFI

skyhigh

netskope

FORNETIX

rsd
Your Information. Governed.

intel

Who has products in the market – SNIA Vendor Large Voting

NetApp

Hitachi Data Systems

RSA
The Security Division of EMC

IBM

DELL
The power to do more

hp

HUAWEI

ORACLE

EMC²

FUJITSU

intel

Key Management – Embedded in major sector products

Storage

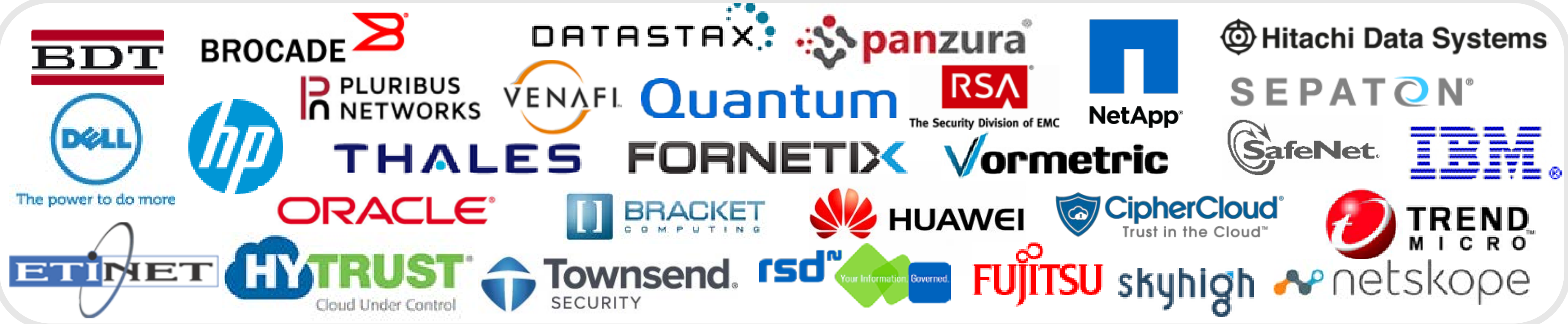
- Disk Arrays, Flash Storage Arrays, NAS Appliances
- Tape Libraries, Virtual Tape Libraries
- Encrypting Switches
- Storage Key Managers
- Storage Controllers
- Storage Operating Systems

Security & Infrastructure

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

Cloud

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



How is enterprise key management being used in storage?

Disk & Flash Arrays, NAS, Storage Operating Systems

- Vaulting master authentication key
- Cluster-wide sharing of configuration settings
- Specific Usage Limits checking (policy)
- FIPS 140-2 external key generation (create, retrieve)
- Multi-version key support during Rekey
- Backup and recover of device specific key sets

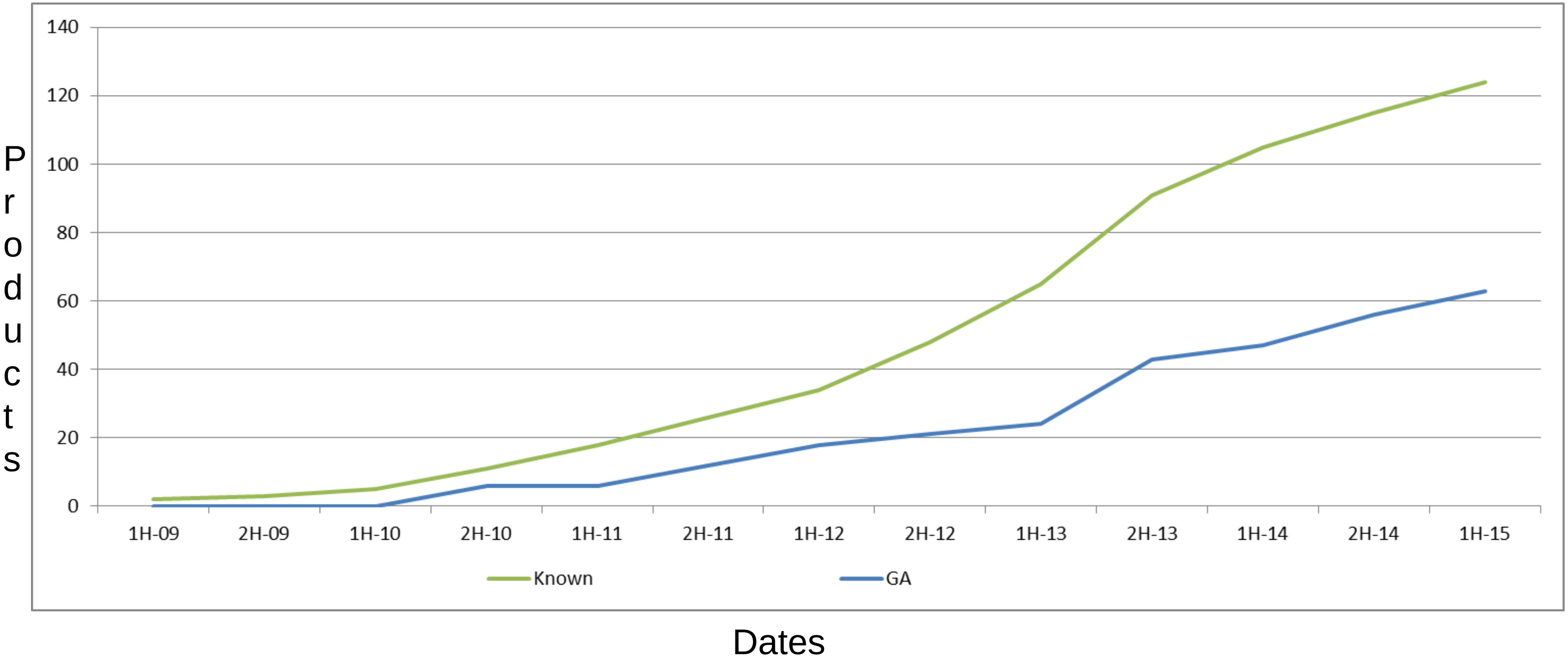
Tape Libraries, Virtual Tape Libraries

- External key generation (create, retrieve)
- FIPS 140-2 external key generation (create, retrieve)
- Multi-version key support during Rekey

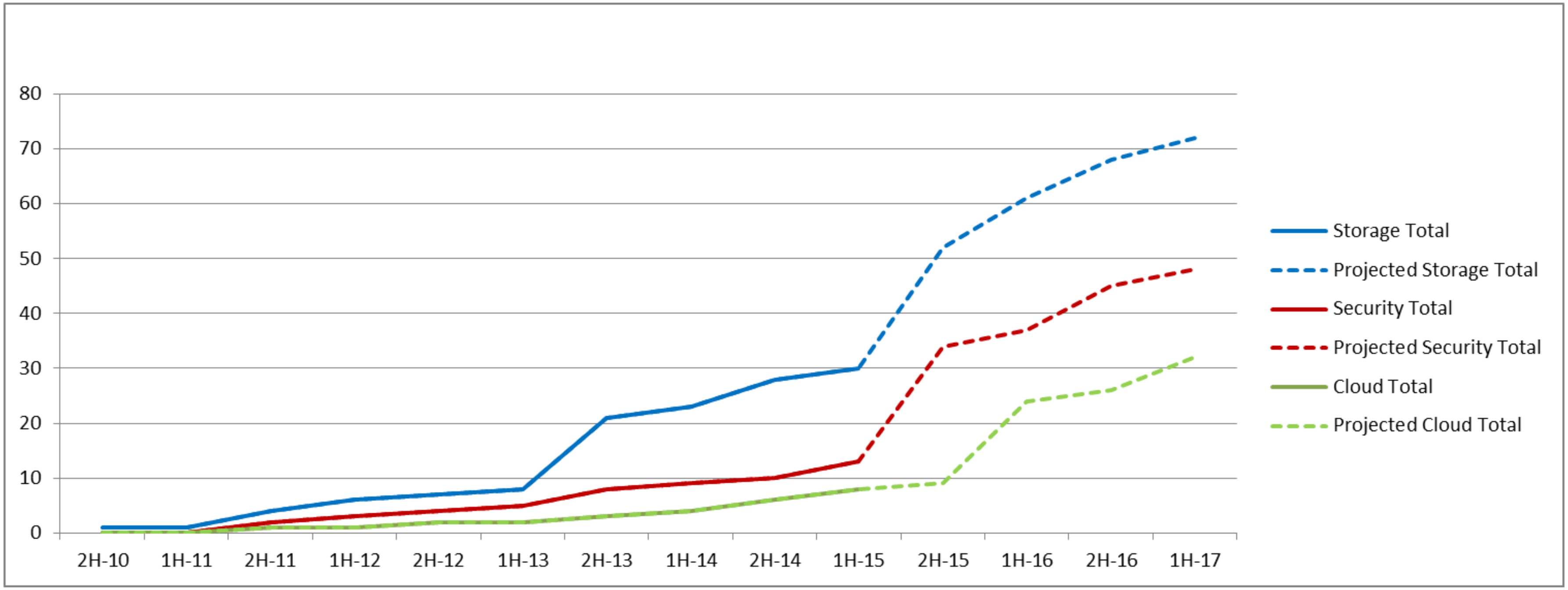
Enterprise Key Management:

Truths: The future market

Generally Available and Known Implementations



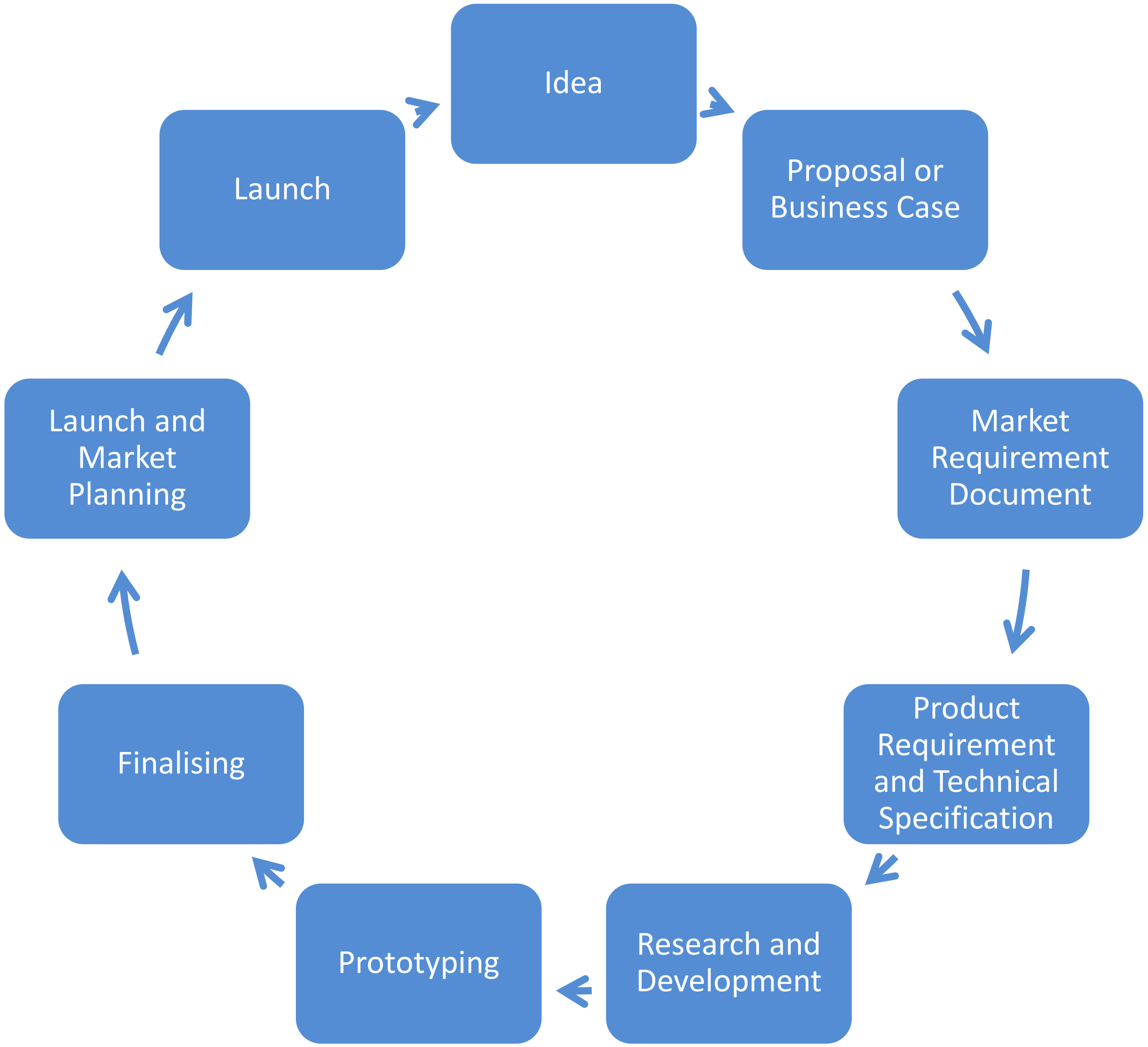
Enterprise Key Management Trends



Enterprise Key Management:

Consequences: The future market

Product Development Cycle



Idea

Proposal or Business Case

Market Requirement Document

Product Requirement and Technical Specification

Research and Development

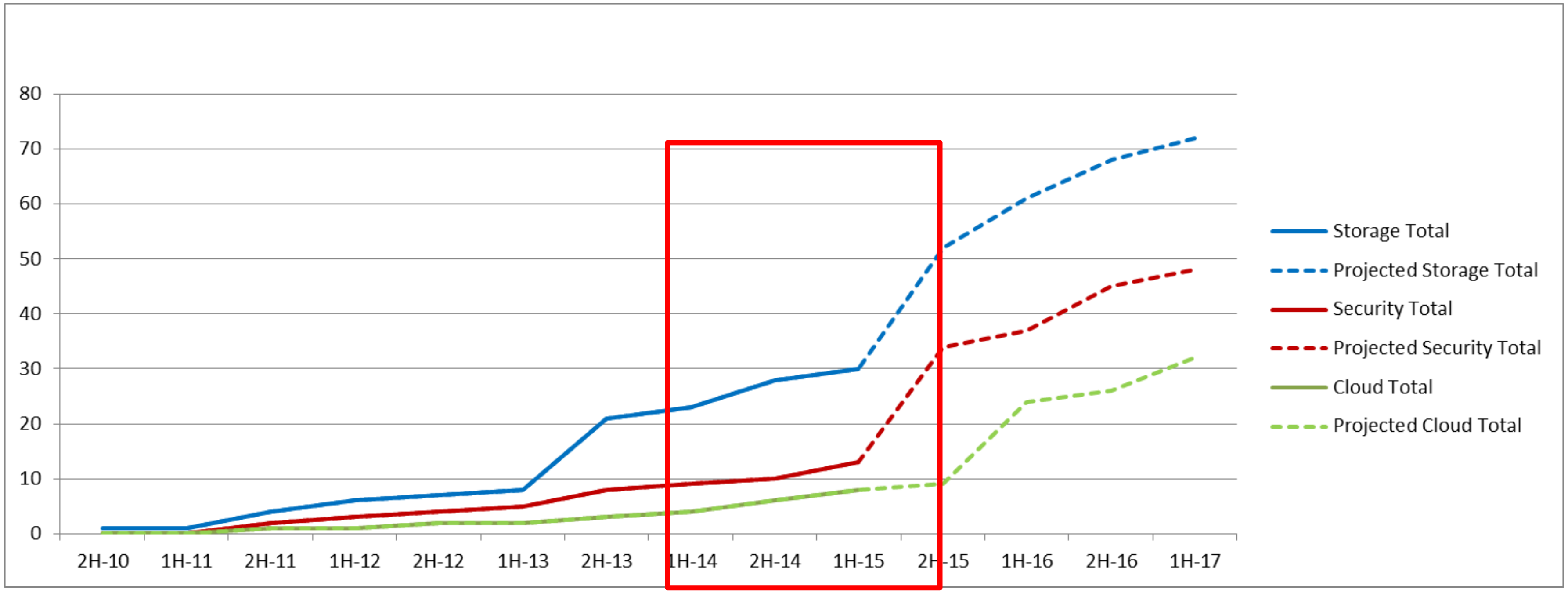
Prototyping

Finalising

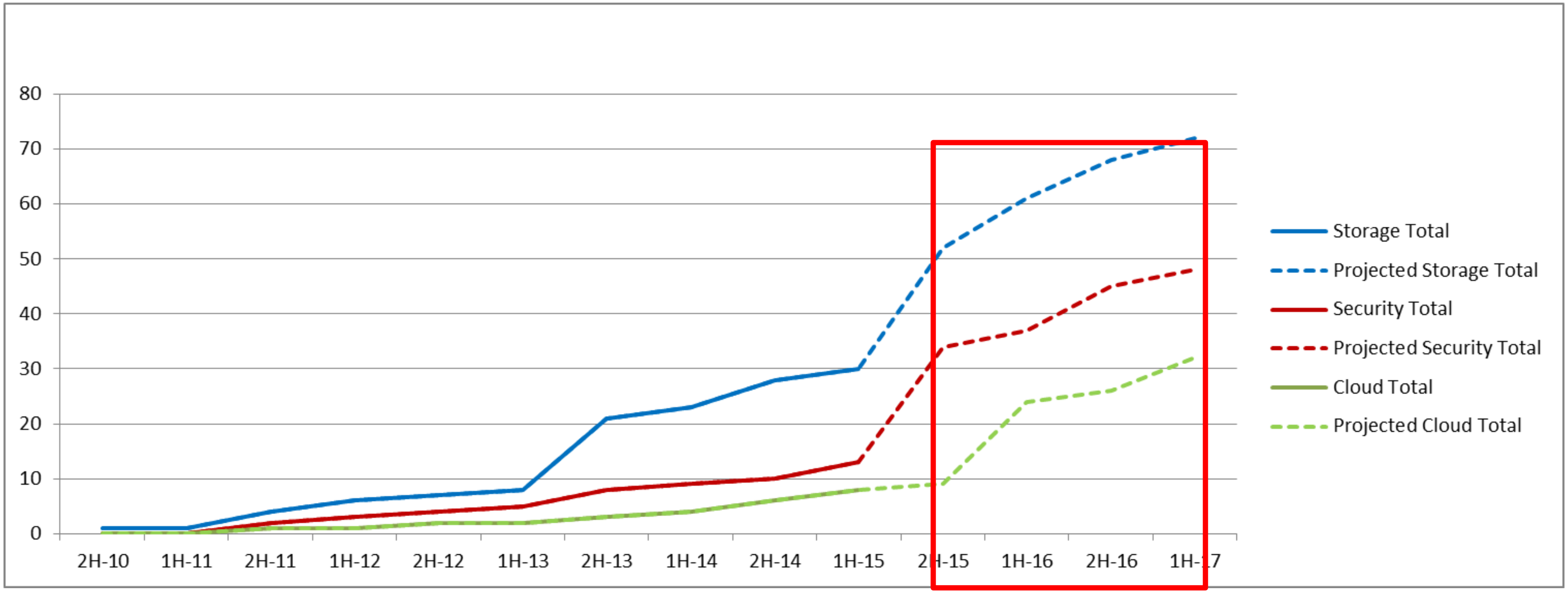
Launch and Market Planning

Launch

Enterprise Key Management - Consequences



Enterprise Key Management - Consequences

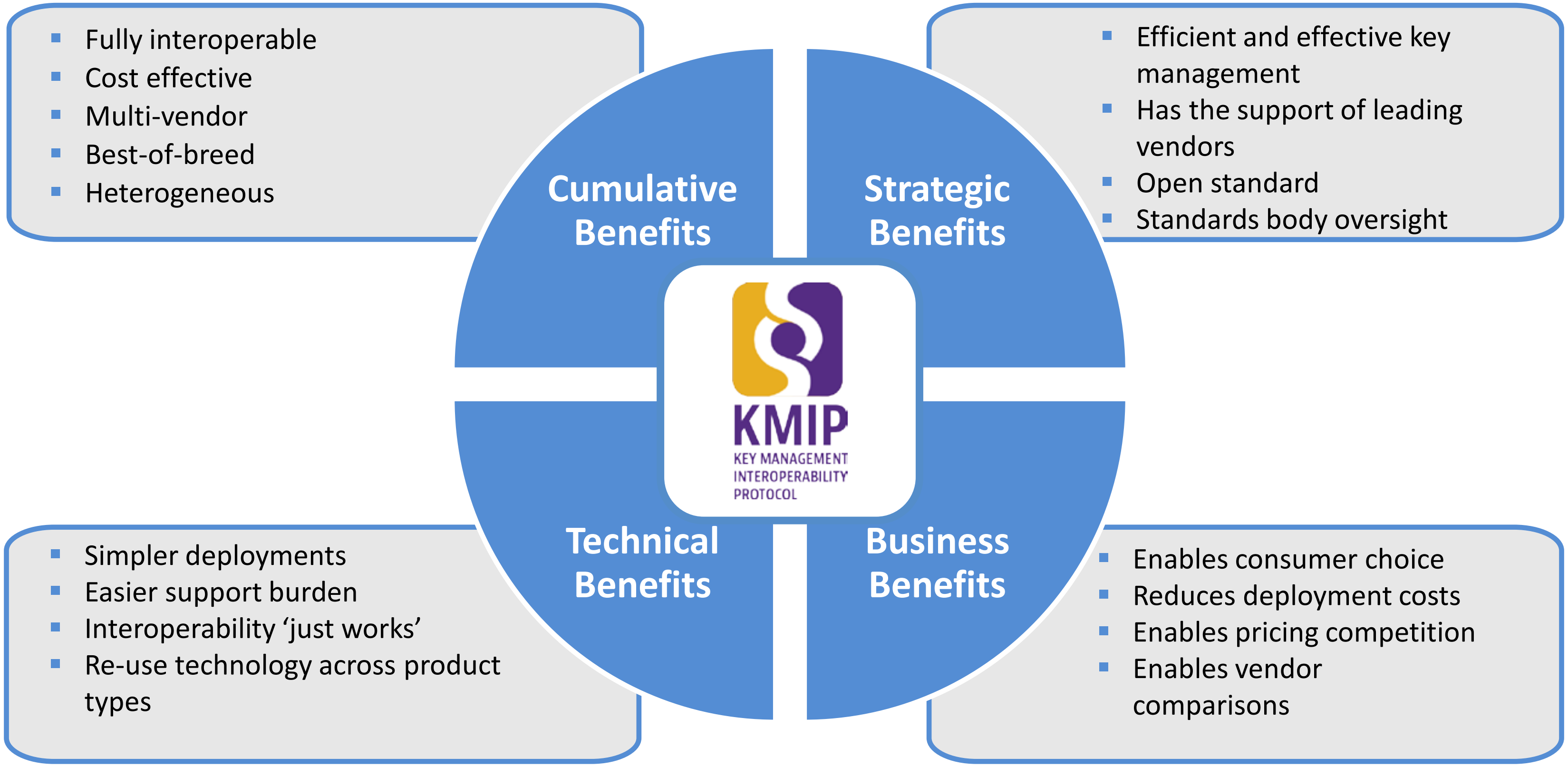


What do the end users want?

Truths of the end-user

010000011010100100101100101010000010101000101001101001111010001100

End-User Requirements



- Fully interoperable
- Cost effective
- Multi-vendor
- Best-of-breed
- Heterogeneous

Cumulative Benefits

Strategic Benefits

- Efficient and effective key management
- Has the support of leading vendors
- Open standard
- Standards body oversight

KMIP

KEY MANAGEMENT INTEROPERABILITY PROTOCOL

Technical Benefits

- Simpler deployments
- Easier support burden
- Interoperability ‘just works’
- Re-use technology across product types

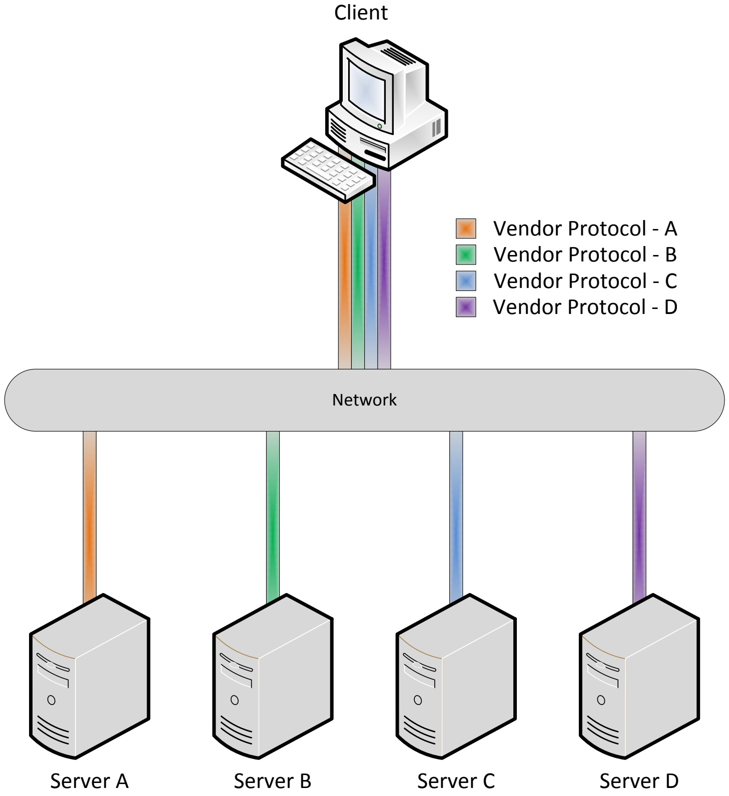
Business Benefits

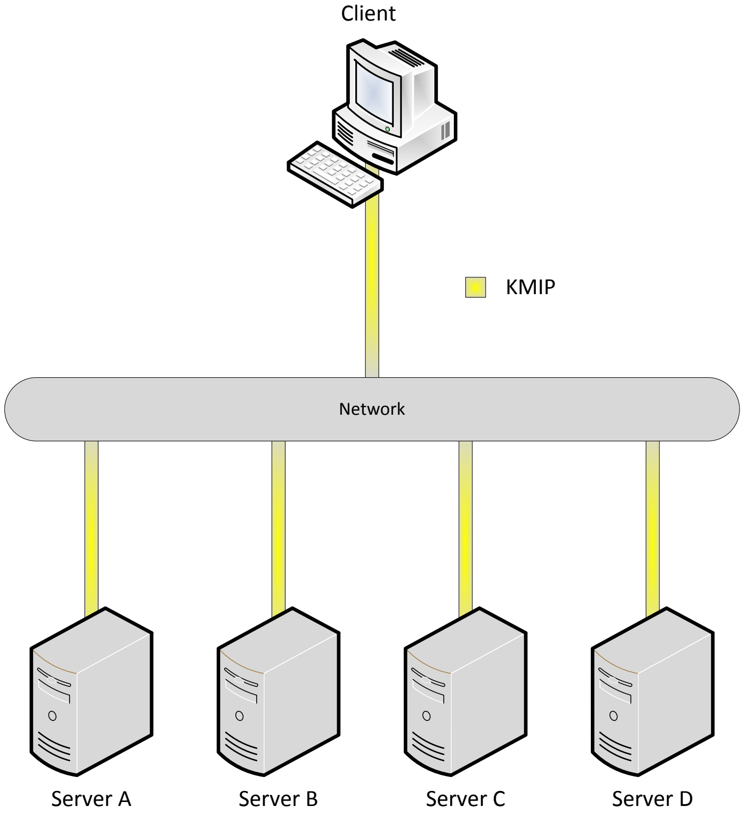
- Enables consumer choice
- Reduces deployment costs
- Enables pricing competition
- Enables vendor comparisons

Choosing a Enterprise Key Manager Vendor

Truths and Consequences

KMIP – Linking Key Management Servers and Clients





Prior to KMIP each application had to support each vendor protocol

With KMIP each application only requires support for one protocol

Choosing a Enterprise Key Manager Vendor

Vendor Commitment to Open Standards

- Does the vendor participate in open key management standards?
- Does the vendor offer an open standard in their currently shipping servers?
- Does the vendor use the open standard in their key management clients?
- Which other security vendors support the open standard if it isn't KMIP?

Vendor Propriety Protocols

- Is the vendor proprietary protocol documented?
- Have customers or other vendors independently implemented the protocol?
- How many variations or versions of the protocol exist and are they forward compatible?
- Which protocol versions are no longer supported?

Choosing a Enterprise Key Manager Vendor

Interoperability

- Does the vendor provide an SDK for application integration?
- Which programming languages are supported: C, Java, C-Sharp, Other?
- For C SDKs, which platforms are supported?
- Is there support for standard Web integration?
- Is source for the SDK provided or able to be purchased?

Key Management Open Standards Contenders

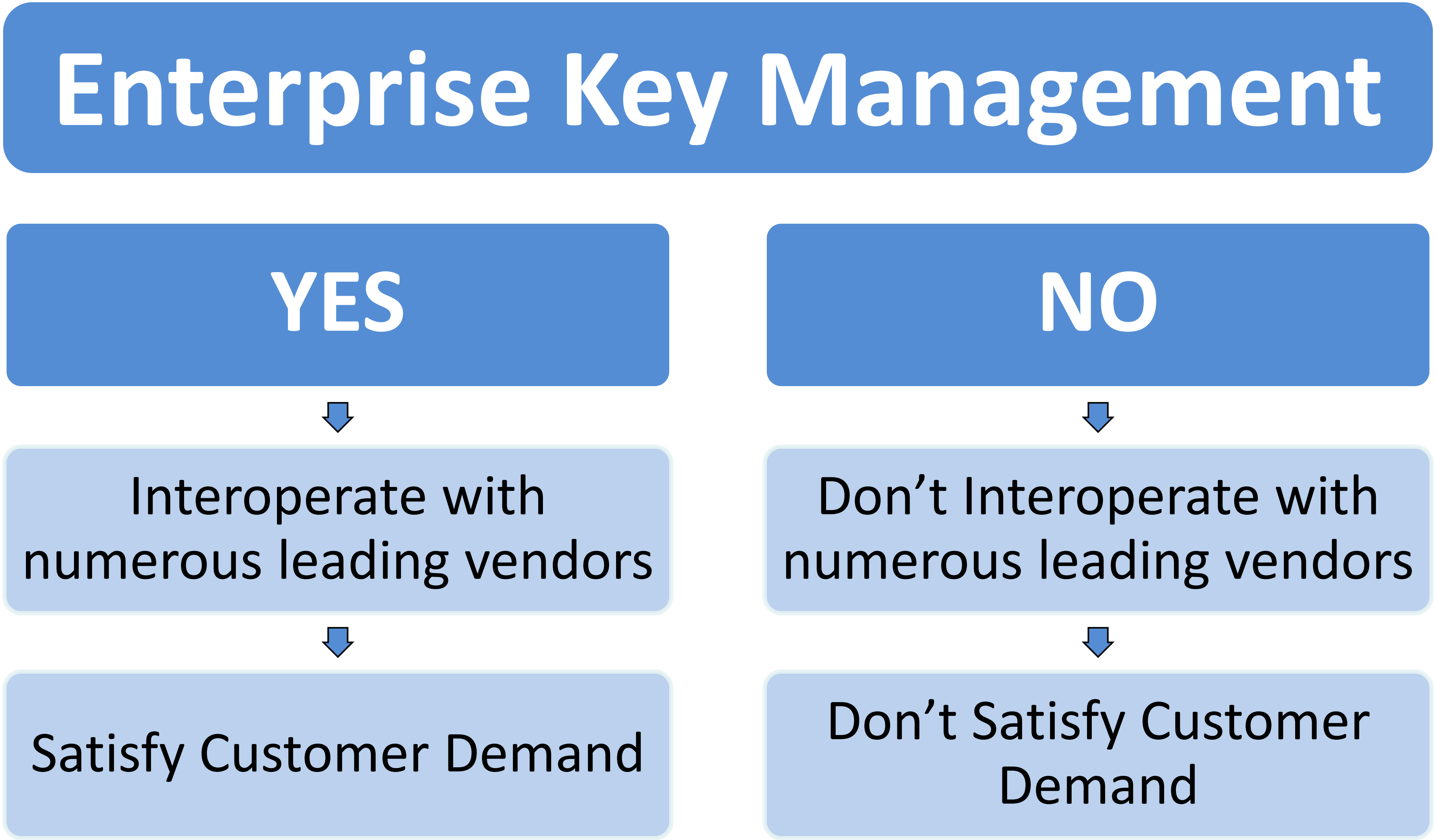
- Does the vendor offer support for KMIP 1.0?
- When will KMIP 1.1 be supported?
- When will KMIP 1.2 be supported?
- Which KMIP profiles are supported?
- When is KMIP 1.3 support planned (in draft)

Choosing a Enterprise Key Manager Vendor

Application Integration

- For the specified standard which other vendors have tested interoperability?
- What functionality was covered by the interoperability testing?
- How was the interoperability testing performed?
- Has independent verification of the testing occurred?
- Can the testing reports be provided for verification?
- Can a customer easily repeat the claimed interoperability testing?
- Are interoperability servers internet accessible for testing?
- Are standard secure Web Proxies supported for navigation of gateways/firewalls?

Consequences – Vendors are chosen or not



Enterprise Key Management

YES

Interoperate with numerous leading vendors

Satisfy Customer Demand

NO

Don’t Interoperate with numerous leading vendors

Don’t Satisfy Customer Demand

KEY MANAGEMENT: Truths and Consequences

Any Questions?

01000011010100100101100101010000010101000101001101001111010001100

- Cryptsoft Pty Ltd
- info@cryptsoft.com
- http://www.cryptsoft.com