FORNETIX

KMIP & PKCS#11 — In Open Standards We Trust and Why You Should Too

PRESENTED BY FORNETIX & UTIMACO

MEET TODAY'S

Presenters

Chuck White

Chief Technology Officer, Fornetix

Richard Williamson

Member of Technical Staff, Utimaco

TODAY'S

Agenda

1. What Is OASIS?
2. Key Management Interoperability Protocol (KMIP)
3. KMIP Applied: Key Orchestration
4. PKCS#11
5. PKCS#11 Applied: Utimaco
6. The Power of Combined Standards
7. Looking Forward

FORNETIX

What Is OASIS?

OASIS is a nonprofit consortium that drives the development, convergence, and adoption of open standards for the global information society.

OASIS works because different teams come to OASIS from different background and different goals.

THE POWER OF

Open Standards

Using standards allows you to:

- Adopt the use of encryption throughout
- Address the market as it is
- Address the market as it changes, adapts, and increases

Security as the foundation of your environment:

- Requires root of trust anchored in hardware
- Standards are the grease in a complex system-of-systems

FORNETIX

OVERVIEW OF

KMIP

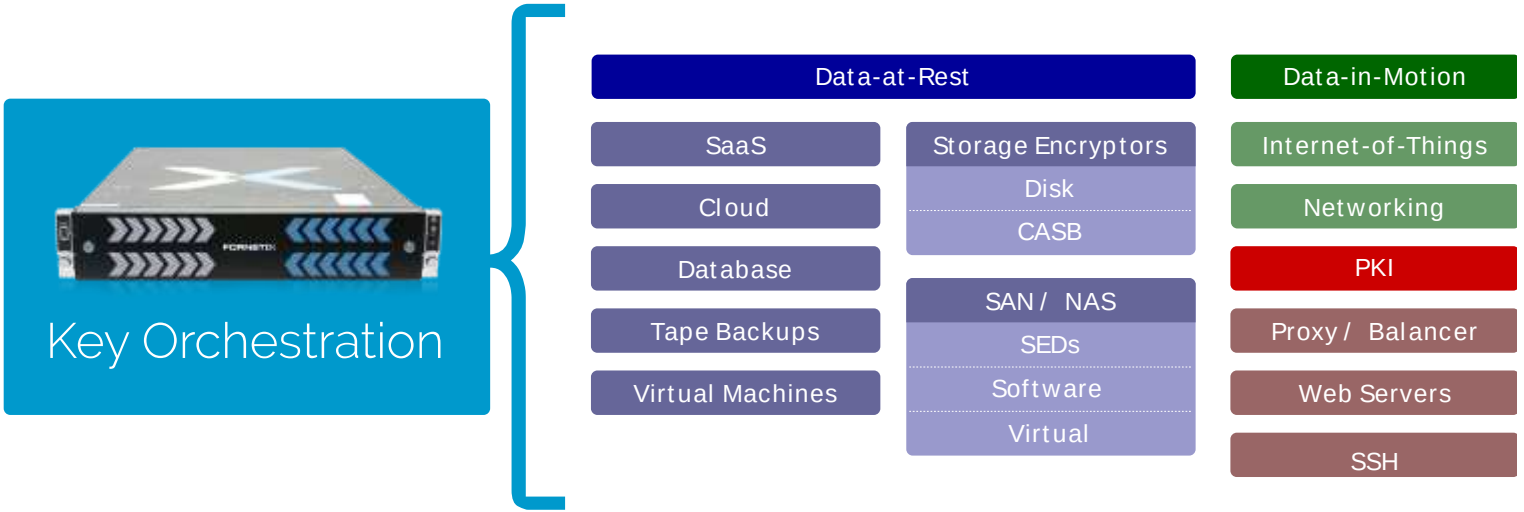
- Key Management Interoperability Protocol was first released in 2010
- Industry Standard for key management with strong support for data-at-rest encryption in storage, backup, and archive solutions
- Emphasis on NIST 800-57 for key lifecycle operations
- Defines the API (XML, JSON, TTLV) and the transport (Mutual TLS)
- KMIP versions 1.0 — 1.4 have been released. Version 2.0 in progress.
- Starting in KMIP 1.2, the capability has been added to support data-in-motion, internet-of-things (IoT), and cloud requirements

OVERVIEW OF

Fornetix & KMIP

Key Orchestration is about applying key management to your business...

Interoperability with extensibility, security, and scale



FORNETIX

OVERVIEW OF

PKCS#11

- The Public Key Cryptography Standard 11 was first released in 1995
- Originally a project of RSA Security, later transitioned to OASIS in 2012
- Industry Standard for encryption tokens, keys, and how they are used
- Defines object types (keys, certificates, etc) and all functions needed:
  - Generate
  - Use
  - Delete
  - Protect
- Versions 1.0, 2.01, 2.10, 2.11, 2.20 and 2.40 published. Version 3.00 is in progress and will add support for IoT and data-in-motion.
- The standard supports “vendor defined mechanisms,” which allows for things like post-quantum cryptography implementations

FORNETIX

OVERVIEW OF

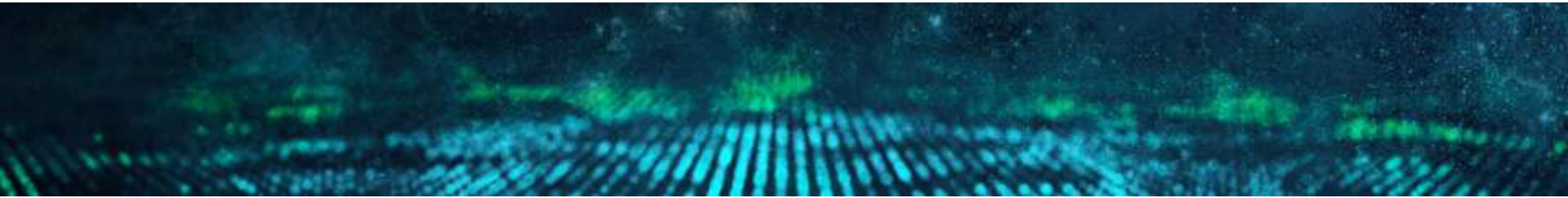
Utimaco & PKCS#11

- Utimaco HSMs have supported PKCS#11 for almost two decades
  - Two major implementations over that time
  - The R2 (current) version has benefited from academic review and subsequent hardening rounds
- Current support is for v2.40, and v3.00 will be available when published by OASIS
  - Important 3.00 behavior is already available (batch mode encryption/decryption)

FORNETIX

USING BOTH STANDARDS FOR A

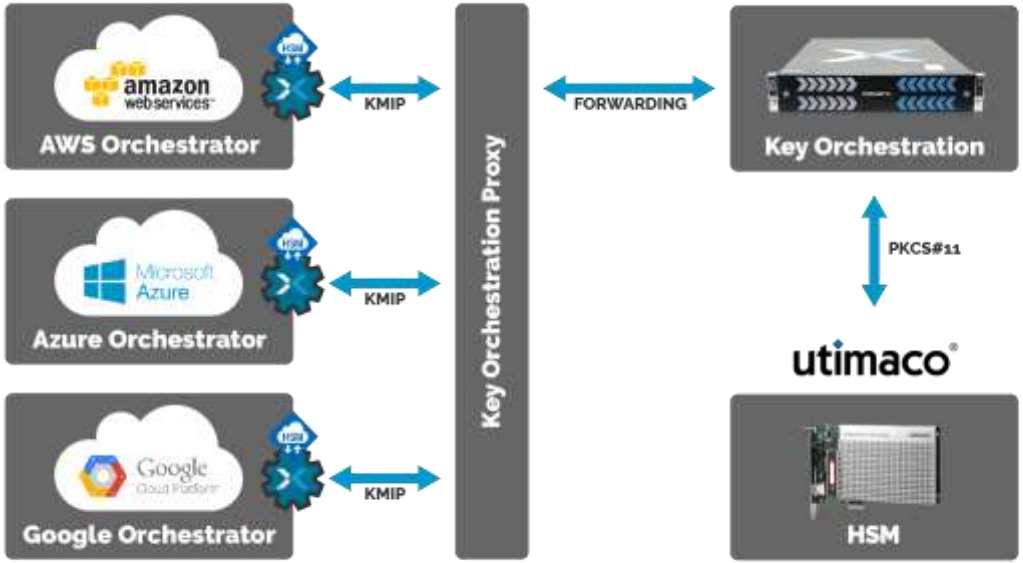
Powerful Combined Solution



- Secure key management enclaves protected by HSMs
- Remote systems that store keys in HSMs
- KMIP for managed key lifecycle, orchestration, governance, and transport
- PKCS11 for resilient enclaves, encryption, decryption, and identity (smart cards and tokens)
- The overlap between standards (in both technologies and people) gives organizations options on how to employ cryptography.

MULTI-CLOUD

Key Management



AWS

Orchestrator provides a KMIP network connection to transport keys into the Utimaco Cloud HSM and management of imported AWS customer master keys

Azure

Orchestrator uses PKCS#11 APIs to register key material from the KO Appliance into Utimaco Cloud HSM

Google

Orchestrator integrates and aligns cloud functions with Utimaco Cloud HSM

Fornetix & Utimaco

The Key Orchestration Appliance provides secure communications channel for enclaves secured with Utimaco Embedded and Cloud HSMs

Utimaco

Embedded or Network HSM protects the Key Orchestration enclave

FORNETIX

OVERVIEW OF

Utimaco & HSMs

- The Utimaco CryptoServer can be used on-prem or in the cloud
- Support for clustering, HA, and FT
- CryptoServers cloud-based key material is accessible from different CSPs — at the same time (create on Azure, sign with AWS, verify using GPC)
- The Utimaco CryptoServer Simulator can be downloaded from our website, hsm.utimaco.com
  - All the software features of the physical hardware, and uses the same host APIs and configuration

FORNETIX

CONTACT

Information

CHUCK WHITE
chuck@fornetix.com

RICHARD WILLIAMSON
richard.williamson@utimaco.com

MORE INFO
Fornetix: www.fornetix.com
Utimaco: hsm.utimaco.com

FORNETIX