
Latest advances in OASIS KMIP and PKCS #11 Encryption and Cryptographic Token Interface Standards Demonstrated by Twelve Companies at RSA 2016

Interoperability Between Cryptosense, Cryptsoft, Feitian, Fometix, Hewlett Packard Enterprise (HPE), IBM, Oracle, P6R, Quintessence Labs, SafeNet, Townsend Security, and Utimaco Products on Display

San Francisco, CA; 29 February 2016 ? The encryption and security community is asking for more from their foundational standards. Developers of the [OASIS Key Management Interoperability Protocol \(KMIP\)](#) [1] and the [Public-Key Cryptography Standard \(PKCS\) #11](#) [2] show how they're rising to that challenge at RSA 2016. In a multi-vendor showcase, 12 vendors demonstrate their support for new features in two of the industry's most widely-adopted security standards.

"The OASIS 2016 Interop is a small window into the reality of proven interoperability between enterprise key managers, HSMs, cryptographic devices, storage, security and cloud products," said Tony Cox, OASIS KMIP Technical Committee Co-Chair and Interoperability Event Lead. "Demonstrating interoperability between these products live at the RSA conference each year reinforces the reality of choice for CIOs, CSOs and CTOs, enabling products from multiple vendors to be deployed as a single enterprise security solution that addresses both current and future requirements."

KMIP Interop

Work in progress on version 1.4 of KMIP, as well as versions 1.3 and 1.2, will show how KMIP enables true interoperable communication between key management clients and key management servers. The RSA demo features clients from Cryptsoft, Fometix, P6R, and Quintessence Labs communicating with key management servers from Cryptsoft, Fometix, HPE, IBM, Quintessence Labs, SafeNet, Townsend Security, and Utimaco. The clients and servers demonstrate the full key management life-cycle including creating, registering, locating, retrieving, deleting, and transferring symmetric and asymmetric keys and certificates between vendor systems.

PKCS #11 Interop

The latest PKCS #11 advances are also featured at RSA. Consumer technologies from Cryptosense, Cryptsoft, and Feitian are communicating with provider technologies from Cryptosense, Cryptsoft, Feitian, Oracle, P6R, Quintessence Labs and Utimaco. Vendor-independent storage of cryptographic information and performance of cryptographic functions are shown, including generating, finding and using cryptographic objects with combinations of one or more symmetric keys, asymmetric keys, or certificates between vendor systems. Here too, booth visitors see multiple versions of PKCS #11 in practice, demonstrating the value the standard for interacting with cryptographic devices in multi-vendor environments.

The OASIS KMIP and PKCS #11 Interops are being held at RSA Conference 2016 in Booth 821 from 29 February to 3 March.

Support for KMIP and PKCS #11 Demos

Cryptsoft

"Encryption and protection of enterprise data is now ubiquitous and interoperability between key management and encryption systems has shifted from a 'nice-to-have' to essential. The OASIS KMIP and PKCS #11 standards are the mechanisms to address the fundamental interoperability requirement enabling migration from single point ad-hoc products to full enterprise security solutions. As a major OEM technology supplier, supplying OASIS conformant solutions helps ensure true interoperability is a reality for our customers."

--*Tim Hudson, CTO, Cryptsoft*

Fornetix

"We at Fornetix are incredibly pleased to see the continued growth in acceptance of both KMIP and PKCS #11. The diverse set of participants are proof positive that the work of OASIS and the KMIP and PKCS #11 Technical Committees are generating real-world solutions for interoperability."

--*Chuck White, CTO, Fornetix*

Gemalto

"With more than 45 documented KMIP integrations, SafeNet KeySecure helps protect data in the most widely deployed IT products and services across the cloud, backup, big data, and storage including Nutanix, MongoDB, Centrify and Commvault. Enterprises benefit from our broad ecosystem of technology partner product integrations that help unify the control of data and improve compliance, all from a centralized key management solution."

--*Steve Kingston, product manager for data protection, Gemalto*

HPE

"As one of the original founders of the KMIP standards community, HPE Security is dedicated to helping our customers and partners accelerate their data protection strategies with our ESKM certified conformant KMIP server, as featured in the OASIS RSA 2016 Interoperability Showcase. Offering one of the industry's broadest portfolio of KMIP-enabled products, HPE also welcomes external partners who support KMIP and provides a Technology Partner Qualification Program to assist them in verifying KMIP interoperability and best practices."

--*Albert Biketi, VP and general manager, HPE Security ? Data Security*

IBM

"IBM is again excited to participate in this year's OASIS Interop at RSA. All of the participants have advanced with the development and implementation of KMIP and we are all excited to show how KMIP adoption continues grow in our industry and the critical value it provides in securing the exchange of encryption keys on premise and in the cloud. On behalf of our customers, IBM brings leadership in intelligence, integration and expertise to data protection through its ongoing contribution to and promotion of this global standard."

--Rick Robinson, *IBM Offering Management, Encryption and Key Management*

Oracle

"Security has always been core to the design of Oracle's products. Oracle Solaris 11 and Oracle SPARC M7 take security to the next level: the revolutionary Silicon Secured Memory capability helps prevent typical attacks like memory over-reads and memory over-writes. The built-in, advanced hardware cryptography provides up to 18 times faster crypto performance compared to x86 processors. Leveraging the OASIS PKCS#11 standard in Oracle Solaris enables developers to take advantage of these capabilities and provides the algorithms needed to build secure applications, databases and programming languages for the cloud."

--Markus Flierl, *VP, Oracle Solaris Core Technology*

About OASIS:

OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit, international consortium that drives the development, convergence and adoption of open standards for the global information society. OASIS promotes industry consensus and produces worldwide standards for security, cloud computing, Web services, the Smart Grid, content technologies, business transactions, emergency management, and other applications. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology. OASIS members broadly represent the marketplace of public and private sector technology leaders, users, and influencers. The consortium has more than 5,000 participants representing over 600 organizations and individual members in 100 countries.

<http://www.oasis-open.org>

Press contact: Carol Geyer carol.geyer@oasis-open.org +1.941.284.0403

Links:

[1] <http://www.oasis-open.org/committees/kmip/>

[2] <http://www.oasis-open.org/committees/pkcs11/>