



Published on OASIS (<https://www.oasis-open.org>)

Latest Advances in OASIS KMIP and PKCS #11 Encryption and Cryptographic Standards Demonstrated by 10 Companies at RSA Conference 2018

Cryptsoft, Foretix, IBM Security, Kryptus, Micro Focus, P6R, Quintessence Labs, Thales eSecurity, Unbound Tech, and Utimaco Demo KMIP Interoperability and/or PKCS #11 Support

16 April 2018 -- At the RSA Conference 2018, members of the OASIS international consortium collaborate to demonstrate their support for new features in two of the industry's most widely-adopted security standards, the Key Management Interoperability Protocol (KMIP) Standard and the Public-Key Cryptography (PKCS) #11 Standard. The demos are being held from 16-19 April, in Booth 1601.

"As the need to encrypt data within the enterprise continues to grow, especially in the face of GDPR and mandatory data breach notice compliance, so too does the need to manage the keys, certificates, and security-relevant information. It is this need that drives the continual evolution of the standards that enable secure and seamless integration of critical cybersecurity tools into the enterprise," said Tony Cox of Cryptsoft, co-chair of the OASIS KMIP and PKCS#11 Technical Committees and Lead for both the KMIP and PKCS11 Interop events. "The demonstration of both the KMIP and PKCS#11 standards provides booth attendees with a clear view of how mainstream products are implementing conformant solutions and showing live interaction between vendor solutions."

KMIP Demonstration

Nine companies are demonstrating the KMIP v2.0 working draft and/or v1.4 current standard. The demo includes interchange of security objects as well as provision of encryption keys and cryptographic services across a common interface. OASIS KMIP Technical Committee members, Cryptsoft, Foretix, IBM Security, Kryptus, Micro Focus, P6R, Quintessence Labs, Thales eSecurity, and Unbound Tech, are participating. Their implementations demonstrate the full key management life-cycle including creating, registering, locating, retrieving, deleting, and transferring symmetric and asymmetric keys and certificates between vendor systems. RSA booth visitors witness live demonstrations of interoperable encryption key and security object management inter-change between every member.

PKCS#11 Showcase

The PKCS#11 3.0 working draft and the PKCS#11 v2.40-errata-01 current standard are being demonstrated by Cryptsoft, Foretix, Quintessence Labs, and Utimaco. Each company showcases their implementation or use of the specification including generating, finding and using cryptographic objects with combinations of one or more symmetric keys, asymmetric keys, or certificates. RSA booth visitors view standalone demonstrations of

key and certificate usage within each of the implementations on display.

Support for KMIP and PKCS #11

Cryptsoft CTO, Tim Hudson, said, "Interoperability between key management, hardware security, and encryption systems is no longer ?nice-to-have? but essential. The OASIS KMIP and PKCS #11 standards provide 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 ensures interoperability is a reality for our customers."

Fornetix CTO, Chuck White, said, "The Fornetix Team is both proud and thankful for the opportunity to participate in OASIS and this year?s KMIP Interop and PKCS11 Showcase. With KMIP, PKCS11 and now OpenC2, OASIS continues to provide a path forward; supporting standards that bring order to the chaos of evolving technology and markets. Our customers need technology that is interoperable ? our support and participation in OASIS demonstrate our commitment to deliver standards-based security to those who need it."

IBM Security WW Offering Manager, Encryption and Key Management, Rick Robinson, said, "IBM is pleased to participate again with other OASIS members at RSA for KMIP-interoperability. Each year we work together as an industry to provide better and more secure key management with greater interoperability amongst all of our products and services. This is not only good for the standard, but it great for our customers who deserve secure, dynamic, and flexible solutions to meet their growing encryption and key management needs."

KRYPTUS CEO, Roberto Gallo, Ph.D., said, "KRYPTUS has been offering Cryptographic Hardware solutions and Cyber Security services since 2003, enabling causes and missions that seek the greater good. Our mission is to provide our customers a secure environment for their operations, keeping them always one step ahead of opponents and threats. For us, security is more than protecting, it is also enabling the new."

P6R CEO, Jim Susoy, said, "As encryption and key management have become commonplace in technology, the importance of interoperable vendor neutral APIs and protocols becomes critical. As a major technology provider, P6R provides conformant KMIP client and server SDKs, KMIP to PKC#11 gateways and PKCS#11 client toolkits. Participating in the OASIS Interop is a great way to help ensure that our solutions are interoperable."

QuintessenceLabs CTO, John Leiseboer, said, "QuintessenceLabs has been involved with OASIS and the KMIP Technical Committee since the beginning, and we pride ourselves on making sure each of our products is compliant via rigorous testing. Interoperability greatly benefits our customers and empowers them in controlling their organization?s security."

Thales eSecurity CTO, Jon Geater, said, "From cloud computing to mobile devices, digital payments, and emerging IoT applications, cryptography is playing an increasingly large role, not only in ensuring data is secure, but also available when needed. As a provider of encryption and key management systems and an originating author of the KMIP specification, Thales is a strong supporter of KMIP to enable enterprises to join the digital world in safety."

Unbound Tech VP of Products, Oz Mishli, said, "KMIP has made impressive strides in encrypted key management and with the accelerating use of cloud-based systems, it?s critical to protect data at every stage. At RSA Conference, as an active partner of the OASIS KMIP Technical Committee, we?re eager to demonstrate the gravity of KMIP?s contributions to cryptographic key management environments such as cost reduction and improved interoperability. We look forward to continuing to help shape the standards that will facilitate interoperation between vendors."

About OASIS:

OASIS is a nonprofit, 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 key management, cryptography, cybersecurity, privacy, cloud computing, IoT, and other areas. 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 65+ countries.

Press contact:

communications@oasis-open.org
