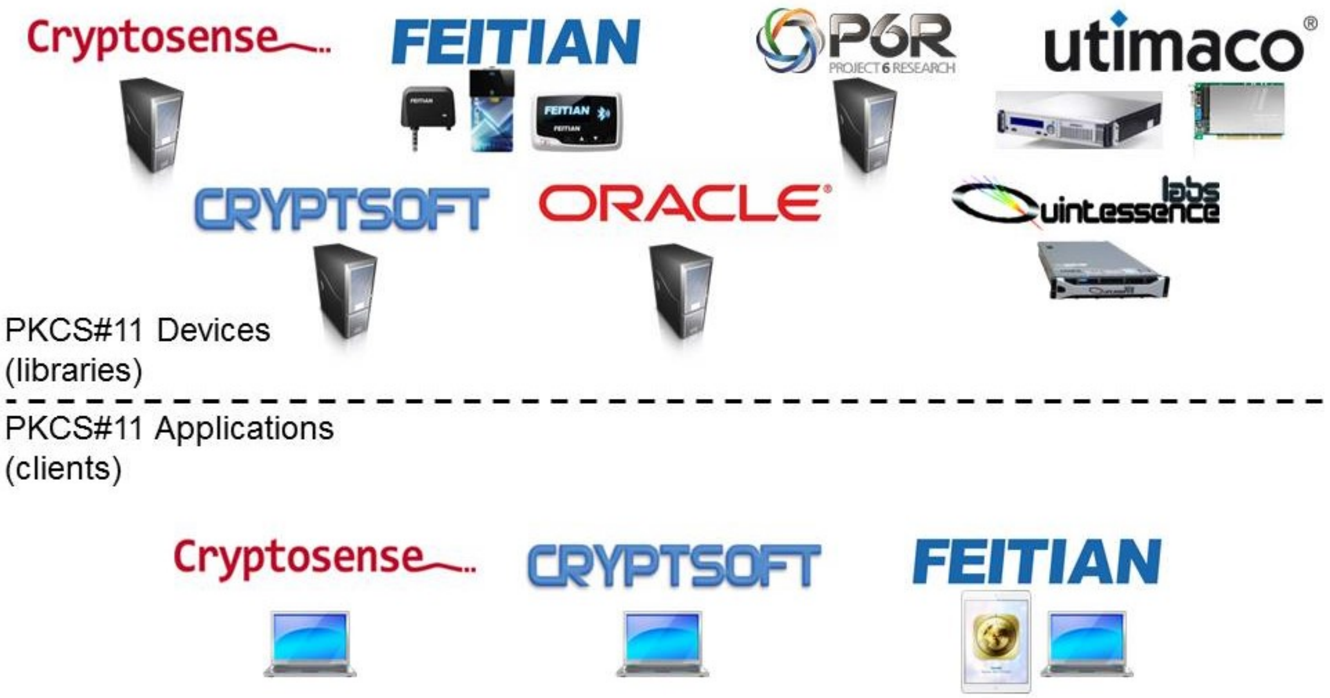
OASIS STANDARD

PKCS #11

Interoperability Demonstration 2016 RSA Conference & Exposition

The latest PKCS #11 advances are featured during this Interop 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.



PKCS#11 Devices (libraries)

PKCS#11 Applications (clients)

"The OASIS 2016 interoperability demonstration 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 PKCS #11 Interop 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."

— Tony Cox of Cryptsoft, PKCS #11 Interop Lead

JOIN

PKCS #11 is part of the OASIS Open Standards Network. OASIS is an international consortium that brings companies, governments, academia, and individuals together to solve communications challenges. All are welcome to join and participate in the evolution of PKCS #11.

PKCS #11 Interop Participants

Cryptosense software discovers vulnerabilities in cryptography. Our technology gives enterprise security teams on-demand analysis and real-time monitoring of vulnerabilities in cryptography on the network, in applications, in services and in cryptographic libraries like PKCS#11. Our unique combination of machine learning, fuzzing and logic-based analysis algorithms hunt systematically for implementation flaws, cryptanalytic vulnerabilities, misconfigurations and insecure use of cryptography. Based in Paris, France and founded in 2013, our clients include top international banks and IT firms. To find out more, visit http://cryptosense.com.

Established in 1996, Cryptsoft is an Australian security firm providing specialist products and services for software and hardware developers in the areas of security system design, deployment, validation and interoperability. Cryptsoft offers a range of software development toolkits to enable the rapid integration of enterprise key management and encryption solutions into applications and systems ranging from embedded platforms through to enterprise class appliances and servers. To find out more, visit www.cryptsoft.com.

Established in 1998, FEITIAN is a public company in China and a trusted leader in the global market for EMV contact and contactless smart cards, payment terminals, and user authentication solutions for secure online banking and transaction security. Our end-to-end turnkey solutions include secure hardware, operating systems, middleware, software application, and services such as personalization and remote lifecycle management. FEITIAN is an essential component in the banking, enterprises, government, and educational institutions throughout the world. To find out more, visit www.ftsafe.com.

With more than 420,000 customers—including 100 of the Fortune 100—and with deployments across a wide variety of industries in more than 145 countries, Oracle offers a comprehensive and fully integrated stack of cloud applications, platform services, and engineered systems. To find out more, visit www.oracle.com.

P6R (www.p6r.com) provides multi-platform solutions to a broad range of businesses. P6R's Secure KMIP Client Toolkit (SKC) provides the full KMIP 1.0, 1.1, 1.2, and 1.3 standards implementations. SKC's multi-layered approach allows developers to use the level of functionality that suits their needs. SKC is available for Linux and Windows. P6R's PKCS 11 Provider (version 2.40) includes: KMIP, software, several HSM tokens. P6R is a member of the OASIS KMIP and PKCS 11 Technical committees. To find out more, visit www.p6r.com.

QuintessenceLabs is a leader in quantum cyber-security, delivering solutions to secure valuable data in-transit, at-rest or in-use. Harnessing quantum science, QuintessenceLabs' products uniquely maximize security, increase ROI from existing assets and reduce data-security management complexities. Our Trusted Security Foundation combines a high speed quantum true random number generator, a powerful vendor neutral key and policy manager, and an embedded secure key store, delivering the strongest basis for your security. To find out more, visit www.quintessencelabs.com.

Utimaco is a leading manufacturer of hardware based security solutions that provide the root of trust to keep cryptographic keys safe, secure critical digital infrastructures and protect high value data assets. Only Utimaco delivers a general-purpose hardware security module (HSM) as a customizable platform to easily integrate into existing software solutions, embed business logic and build secure applications. For more information, visit https://hsm.utimaco.com.