OASIS Enhances Popular Public-Key Cryptography Standard, PKCS #11, for Mobile and Cloud

26 March 2013 - More than 25 organizations are partnering at the OASIS open standards consortium to adapt the Public-Key Cryptography Standard, PKCS #11, for mobile and cloud applications. One of the most widely implemented cryptography standards in the world, PKCS #11 specifies a platform-independent application programming interface (API) for cryptographic tokens which store and control authentication information including personal identity, cryptographic keys, certificates, digital signatures, and biometric data.

"We're updating PKCS #11 to address recent advances in cryptography, such as new algorithms. We'll also be considering requirements brought on by mobile devices, cloud computing and virtualization architectures, Web sensors, and contactless payment technologies," said Robert Griffin of RSA, the security division of EMC. Griffin co-chairs the new OASIS PKCS 11 Technical Committee, along with Valerie Fenwick of Oracle.

"By continuing to grow the PKCS #11 standard, we can strengthen support for additional cryptographic algorithms and cryptographic technologies industry wide. We expect the OASIS PKCS Technical Committee will help expand and energize the community of developers, users, and enterprise customers that rely on cryptographic communications and services to secure their tools, applications and data at rest," added Fenwick.

Members of the OASIS PKCS Technical Committee will work to strengthen support for hardware security modules, smart card interfaces, one-time passwords, certificate distribution, and wireless/sensor applications that use near field communication (NFC), RFID, Bluetooth, and Wi-Fi.

PKCS #11 is part of the PKCS family of standards which define data types and functions available to applications using the Cryptoki API. PKCS #11 has been contributed to the OASIS PKCS 11 Technical Committee by RSA, which originally developed and published the standard.

"Increasingly, we see governments and industries passing regulations that mandate the use of encryption to mitigate risks associated with data breaches," noted Laurent Liscia, OASIS executive director and CEO. "We're excited by the opportunity to extend this comprehensive, time-proven PKCS #11 standard for even greater use in protecting data in the mobile and cloud space."
New members are encouraged to join the OASIS PKCS 11 Technical Committee at any time. Archives of the work are accessible to both members and non-members, and OASIS invites public review and comment on the work.

Support for OASIS PKCS 11

Cryptsoft [1]
"As one of the most experienced implementers and integrators of cross-platform PKCS #11 components, Cryptsoft is committed to providing our OEM customers with standards-based technologies and are pleased to support PKCS 11 within OASIS. Building on the solid foundation established by RSA Labs under the PKCS program, the broad vendor support within OASIS will enable further evolution of PKCS #11 to address the full spectrum of requirements of application integration of security devices."
-- Tim Hudson, Chief Security Architect

EMC/RSA [2]
"RSA is excited to have such strong industry support for bringing the PKCS #11 standard into OASIS. This revitalized PKCS #11 effort will provide important improvements to the Cryptoki standard, enabling PKCS #11 to better address important additional technology areas, such as mobile security, where a robust cryptographic API is of critical importance."
-- Robert Philpott, EMC Senior Technologist

Futurex [3]
"The role of data security in today’s technology environment is rapidly expanding. With the inter-national emergence of mobile and cloud-based infrastructure, the number of electronic devices requiring encryption of sensitive information has dramatically grown. PKCS #11 has proven to be a versatile, interoperable standard simplifying the protection of this data. Futurex is committed to advancing industry standards and is pleased to take part in the OASIS initiative to strengthen and diversify PKCS #11."
-- Ryan Smith, Chief Solutions Architect

Oracle [4]
"PKCS #11 is valued for helping keep transactions and data secure. It is imperative that the standard evolve along with the latest IT deployment strategies. As part of our commitment to helping organizations secure their systems and extend the value of their IT investments, we look forward to contributing to the advancements in PKCS #11 to address the increasing number of application requirements related to mobile and cloud."
-- Don Deutsch, VP, Chief Standards Officer

SafeNet [5]
"SafeNet has always promoted interoperability and standards so that customers have choice and simplicity in adopting cryptography solutions. SafeNet is excited to join with other security innovators in the OASIS effort to advance PKCS#11 to meet the cryptographic architectures and requirements for mobile, cloud and virtual environments. Updating the specification to meet the challenges of these rapidly evolving environments will help accelerate their security and adoption."
-- Doron Cohen, VP, Technology, Office of the CTO

SecureAuth [6]
"With the proliferation of cloud and mobile applications, the cryptographic API standard needs to be extended and advanced. Currently, weaknesses are prevalent in identity mechanisms, and often perpetuated due to the difficulty of adopting better designs. Cryptographic identities can achieve better security. Re-invigorating PKCS #11 is a step toward a broader awareness and adoption of the cryptographic identity mechanisms that SecureAuth deploys to millions of users. We are pleased to be a member of this important consortium."
"PKCS #11 provides an important contribution to the security industry by enabling developers to take advantage of proven cryptographic implementations. Developers can choose between an array of assurance levels, from basic software libraries to tamper resistant devices such as hardware security modules (HSMs) that protect keys and the processes that use them. As PKCS #11 expands to address mobile, cloud and virtualized environments, the ability to deploy appropriate levels of security and migrate to higher levels of assurance will be increasingly valuable."

-- Richard Moulds, VP Strategy

"With cloud computing and mobile devices challenging enterprises' ability to control the trust established by cryptographic keys and certificates, PKCS #11 becomes more important than ever. As an evolving OASIS standard, PKCS #11 will enable more organizations to enforce policies and automate operations for an increasing number of keys and certificates, thereby reducing the risk enterprises face from attacks, outages and failed compliance. Venafi looks forward to taking a leadership role in expanding PKCS #11."

-- Paul Turner, VP Product and Customer Solutions

Additional information

OASIS PKCS 11 Technical Committee

About OASIS

OASIS 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, privacy, cloud computing, content technologies, business transactions, energy, emergency management, 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 100 countries.

Press contact

Carol Geyer
OASIS Senior Director, Communications
carol.geyer@oasis-open.org
+1.941.284.0403