OASIS Approves Two Public-Key Cryptography Standards to Advance Post-Quantum Security and Interoperability

Cryptsoft, Entrust Security, IBM, Oracle, Red Hat, and Others Strengthen Security Across Cloud and Hardware Environments

BOSTON, MA, UNITED STATES, July 15, 2026 /EINPresswire.com/ -- OASIS Open, the international open source and standards consortium, announced that PKCS #11 Specification Version 3.2 and PKCS #11 Profiles Version 3.2 have been approved as OASIS Standards. This milestone reflects the highest level of ratification and strengthens the widely deployed Cryptoki (cryptographic token interface) API, which underpins hardware security modules (HSMs), smart cards, and certificate authority systems worldwide.

As organizations face escalating cyber threats alongside the anticipated impact of quantum computing, the PKCS #11 Specification Version 3.2 introduces support for post-quantum cryptographic (PQC) mechanisms along with extended interface capabilities and improved vendor extensions. PKCS #11 Profiles Version 3.2 defines the conformance clauses necessary for consistent, interoperable implementations across vendors and deployment environments.

The OASIS PKCS #11 Technical Committee (TC) said, "Version 3.2 delivers a stronger, cleaner Cryptoki interface and gives implementers a clear, interoperable foundation for addressing emerging threats while maintaining compatibility with existing security infrastructure. As the cryptographic landscape shifts, PKCS #11 remains the stable core that real-world deployments depend on."

The PKCS #11 TC encourages global collaboration and actively seeks input from stakeholders to ensure the success of PKCS #11 as a cornerstone for cryptographic services. The TC welcomes a diverse range of contributors, including architects, designers and implementers. Participation is open to all through OASIS membership; interested parties are encouraged to join and help shape the future of cryptographic interoperability and post-quantum security. Contact join@oasis-open.org for more information.

PKCS #11 is already embedded in the security infrastructure of organizations worldwide. Version 3.2 builds on that proven foundation, giving implementers and vendors a clear path to post-quantum readiness without disrupting existing deployments. The updated files are available in the library as freely accessible OASIS Standards.

Support for PKCS #11

IBM
"IBM has adopted the PKCS#11 v3.2 standard offering exciting new features to protect against quantum computing attacks. API users can leverage openCryptoki, an IBM supported open-source project, which now includes PQC algorithm support with version 3.27."
– Joe Livingston, IBM, EP11 SW Dev. Engineer, Project Lead

Entrust Security
“PKCS #11 provides an important contribution to the security industry by enabling developers to leverage trusted cryptographic implementations. With post quantum computing close on the horizon, standards-based access to secure cryptography has never been more important. Entrust has long supported open standards, supporting PKCS #11 since launching its first nShield HSM in 1998. We value its seamless integration between HSMs and applications and are pleased to support the ratification of PKCS #11 version 3.2.”
– Hamish Cameron, Senior Manager Software Development, Entrust, Data Protection Solutions

About OASIS Open
One of the most respected, nonprofit open source and open standards bodies in the world, OASIS advances the fair, transparent development of open source software and standards through the power of global collaboration and community. OASIS is the home for worldwide standards in AI, emergency management, identity, IoT, cybersecurity, blockchain, privacy, cryptography, cloud computing, urban mobility, and other content technologies. Many OASIS standards go on to be ratified by de jure bodies and referenced in international policies and government procurement. www.oasis-open.org

Media Inquiries: communications@oasis-open.org

Mary Beth Minto
OASIS Open
email us here

in today's world. Please see our Editorial Guidelines for more information.