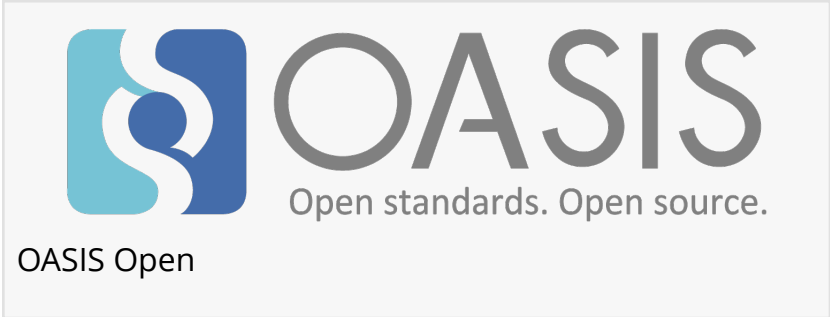
# OASIS Approves Four Public-Key Cryptography (PKCS) #11 Standards

*Cisco, Cryptsoft, Dell, Fornetix, nCipher, Oracle, P6R, Red Hat, and Others Advance Widely Used Authentication Standards*



OASIS Open

BOSTON, MA, USA, July 30, 2020 /EINPresswire.com/ -- The OASIS international open standards consortium today announced that its members have approved four standards to enhance Public-Key Cryptography Standard (PKCS) #11, one of the most widely implemented cryptography standards in the world. The PKCS #11 standards are Version 3.0, and are now official OASIS Standards, a status that signifies the highest level of ratification.

> The approved PKCS #11 standards address the advances in cryptography by including new functions and mechanisms to protect data in the mobile and cloud space."
>
> *Robert Relyea , co-chair of the OASIS PKCS #11 Technical Committee*

PKCS #11, part of the PKCS family of standards, specifies a platform-independent application programming interface (API) for cryptographic tokens, such as hardware security modules and smart cards, which store and control authentication information, including personal identity, cryptographic keys, certificates, digital signatures, and biometric data. The API itself is named "Cryptoki" (from "cryptographic token interface" and pronounced as "crypto-key").

The four approved PKCS #11 standards include:

- PKCS #11 Cryptographic Token Interface Base Specification Version 3.0, known as "Base Specification," defines data types, functions, and other basic components of the PKCS #11 Cryptoki interface.

- PKCS #11 Cryptographic Token Interface Profiles Version 3.0, known as "Profiles," is intended for developers and architects who wish to design systems and applications that conform to the PKCS #11 Cryptographic Token Interface standard.

- PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 3.0, known

as "Current Mechanisms," defines mechanisms that are anticipated for use with the current version of PKCS #11.

PKCS #11 Cryptographic Token Interface Historical Mechanisms Specification Version 3.0, known as "Historical Mechanisms," defines mechanisms for PKCS #11 that are no longer in general use.

"The approved PKCS #11 standards address the advances in cryptography by including new functions and mechanisms to protect data in the mobile and cloud space," said Robert Relyea of Red Hat, co-chair of the OASIS PKCS #11 Technical Committee. "The standard is valued for helping keep transactions and data secure and has adapted to the latest IT deployment strategies."

"We are pleased that the PKCS #11 standard continues to evolve, strengthening support for additional cryptographic algorithms and cryptographic technologies industry-wide," added OASIS PKCS #11 co-chair, Tony Cox of Cryptsoft. "PKCS #11 is a versatile, interoperable standard that enables the secure and seamless integration of critical cybersecurity tools into the enterprise."

Support for PKCS #11

Cryptsoft
"Cryptsoft has been a long-term supplier of cryptographic toolkits for many years and our commitment to the standardization of cryptographic technologies remains resolute. As our society continues to increase its use of cryptographic capabilities, the need to ensure cleaner, more consistent integrations also increases. The release of v3.0 of the PKCS #11 specification raises the bar further and is the culmination of years of hard work by the Technical Committee members towards ensuring that the standard continues to meet today's requirements."
-- Tony Cox, VP Partners Alliances & Standards, Cryptsoft

nCipher
"In our hyper-connected world, standards-based access to secure cryptography has never been more important.  nCipher, an Entrust Datacard company, is a strong advocate of open standards and has continued to support PKCS #11 since 1998 with the first release of its nShield HSM. We value the out-of-the-box integration it brings between our HSMs and vendor applications and are excited by the ratification of PKCS #11 v3.0. We look forward to enabling application vendors to take advantage of the new mechanisms and functions."
-- Kevin McKeogh, Vice President Product Management, nCipher, an Entrust Datacard Company

P6R
"P6R believes in standards and will continue to support the PKCS #11 standard in our PKCS #11 SDK's, KMIP token and AWS CloudHSM products."
-- Jim Susoy, CEO, P6R Inc.

Additional Information
OASIS PKCS #11 Technical Committee: https://www.oasis-open.org/committees/pkcs11

About OASIS
One of the most respected, member-driven standards bodies in the world, OASIS offers projects—including open source projects—a path to standardization and de jure approval for reference in international policy and procurement. OASIS members include major multinational companies, SMEs, government agencies, universities, research institutions, consulting groups, and individuals are represented.

Media Inquiries:

Carol Geyer
OASIS Open
+1 941-284-0403
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn

---