

What is PKCS?

Written by Alexei Spirin

Wednesday, 09 January 2008 21:31 - Last Updated Sunday, 23 May 2010 13:12

The Public-Key Cryptography Standards are specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide for the purpose of accelerating the deployment of public-key cryptography. In other words we use these standards when we work with public key cryptography in general and especially with digital certificates.

- PKCS #1: RSA Cryptography Standard
- PKCS #3: Diffie-Hellman Key Agreement Standard
- PKCS #5: Password-Based Cryptography Standard
- PKCS #6: Extended-Certificate Syntax Standard
- PKCS #7: Cryptographic Message Syntax Standard
- PKCS #8: Private-Key Information Syntax Standard
- PKCS #9: Selected Attribute Types
- PKCS #10: Certification Request Syntax Standard
- PKCS #11: Cryptographic Token Interface Standard
- PKCS #12: Personal Information Exchange Syntax Standard
- PKCS #13: Elliptic Curve Cryptography Standard
- PKCS #15: Cryptographic Token Information Format Standard

[Wiki article](#)

[RSA Lab page](#)