Wikipedia
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

Languages
Čeština
Deutsch
Español
Français
한국어
Italiano
日本語
Polski
Русский
Tiếng Việt
中文
Edit links

PKCS

From Wikipedia, the free encyclopedia

In cryptography, **PKCS** stands for "Public Key Cryptography Standards". These are a group of **public-key cryptography standards** devised and published by RSA Security Inc, starting in the early 1990s. The company published the standards to promote the use of the cryptography techniques to which they had patents, such as the RSA algorithm, the Schnorr signature algorithm and several others. Though not industry standards (because the company retained control over them), some of the standards in recent years[when?] have begun to move into the "standards-track" processes of relevant standards organizations such as the IETF and the PKIX working-group.

PKCS Standards Summary

	Version	Name	Comments
PKCS #1	2.2	RSA Cryptography Standard[1]	See RFC 3447. Defines the mathematical properties and format of RSA public and private keys (ASN.1-encoded in clear-text), and the basic algorithms and encoding/padding schemes for performing RSA encryption, decryption, and producing and verifying signatures.
PKCS #2	-	*Withdrawn*	No longer active as of 2010. Covered RSA encryption of message digests; subsequently merged into PKCS #1.
PKCS #3	1.4	Diffie–Hellman Key Agreement Standard[2]	A cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.
PKCS #4	-	*Withdrawn*	No longer active as of 2010. Covered RSA key syntax; subsequently merged into PKCS #1.
PKCS #5	2.0	Password-based Encryption Standard[3]	See RFC 2898 and PBKDF2.
PKCS #6	1.5	Extended-Certificate Syntax Standard[4]	Defines extensions to the old v1 X.509 certificate specification. Obsoleted by v3 of the same.

PKCS #7	1.5	Cryptographic Message Syntax Standard[5]	See RFC 2315. Used to sign and/or encrypt messages under a PKI. Used also for certificate dissemination (for instance as a response to a PKCS #10 message). Formed the basis for S/MIME, which is as of 2010 based on RFC 5652, an updated Cryptographic Message Syntax Standard (CMS). Often used for single sign-on.
PKCS #8	1.2	Private-Key Information Syntax Standard[6]	See RFC 5958. Used to carry private certificate keypairs (encrypted or unencrypted).
PKCS #9	2.0	Selected Attribute Types[7]	See RFC 2985. Defines selected attribute types for use in PKCS #6 extended certificates, PKCS #7 digitally signed messages, PKCS #8 private-key information, and PKCS #10 certificate-signing requests.
PKCS #10	1.7	Certification Request Standard[8]	See RFC 2986. Format of messages sent to a certification authority to request certification of a public key. See certificate signing request.
PKCS #11	2.40	Cryptographic Token Interface[9]	Also known as "Cryptoki". An API defining a generic interface to cryptographic tokens (see also Hardware Security Module). Often used in single sign-on, public-key cryptography and disk encryption[10] systems. RSA Security has turned over further development of the PKCS #11 standard to the OASIS PKCS 11 Technical Committee.
PKCS #12	1.1	Personal Information Exchange Syntax Standard[11]	See RFC 7292. Defines a file format commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key. PFX is a predecessor to PKCS #12. This container format can contain multiple embedded objects, such as multiple certificates. Usually protected/encrypted with a password. Usable as a format for the Java key store and to establish client authentication certificates in Mozilla Firefox. Usable by Apache Tomcat.

PKCS #13	–	Elliptic Curve Cryptography Standard	*(Apparently abandoned, only reference is a proposal from 1998.)*[12]
PKCS #14	–	Pseudo-random Number Generation	*(Apparently abandoned, no documents exist.)*
PKCS #15	1.1	Cryptographic Token Information Format Standard[13]	Defines a standard allowing users of cryptographic tokens to identify themselves to applications, independent of the application's Cryptoki implementation (PKCS #11) or other API. RSA has relinquished IC-card-related parts of this standard to ISO/IEC 7816-15.[14]

See also [edit]

- Cryptographic Message Syntax

References [edit]

1. ^ "PKCS #1: RSA Cryptography Standard". RSA Laboratories.
2. ^ "PKCS #3: Diffie-Hellman Key Agreement Standard". RSA Laboratories.
3. ^ "PKCS #5: Password-Based Cryptography Standard". RSA Laboratories.
4. ^ "PKCS #6: Extended-Certificate Syntax Standard". RSA Laboratories.
5. ^ "PKCS #7: Cryptographic Message Syntax Standard". RSA Laboratories.
6. ^ "PKCS #8: Private-Key Information Syntax Standard". RSA Laboratories.
7. ^ "PKCS #9: Selected Attribute Types". RSA Laboratories.
8. ^ "PKCS #10: Certification Request Syntax Standard". RSA Laboratories.
9. ^ "PKCS #11: Cryptographic Token Interface Standard". RSA Laboratories.
10. ^ Security Token/Smartcard Support in FreeOTFE
11. ^ "PKCS #12: Personal Information Exchange Syntax Standard". RSA Laboratories. Archived from the original on April 1, 2014.
12. ^ "PKCS #13: Elliptic Curve Cryptography Standard". RSA Laboratories.
13. ^ "PKCS #15: Cryptographic Token Information Format Standard". RSA Laboratories.
14. ^ RSA Laboratories: "PKCS #15: Cryptographic Token Information Format Standard".

General

- Jean-Sébastien Coron, Marc Joye, David Naccache, and Pascal Paillier (2000). "New Attacks on PKCS #1 v1.5 Encryption" (PDF). EUROCRYPT. p. 369–381.

External links [edit]

- RSA Security's page on PKCS
  - What is PKCS? (chapter 5.3.3 of PKCS)
  - About PKCS (appendix G from RFC 3447)
  - OASIS PKCS 11 TC (technical committee home page)

V · T · E **PKCS**

PKCS #1 · PKCS #2 · PKCS #3 · PKCS #4 · PKCS #5 · PKCS #6 · PKCS #7 · PKCS #8 · PKCS #9 · PKCS #10 · PKCS #11 · PKCS #12 · PKCS #13 · PKCS #14 · PKCS #15

V · T · E **Cryptography** [show]

Categories: Cryptography standards | Public-key cryptography

Privacy policy About Wikipedia Disclaimers Contact Wikipedia Developers Cookie statement

Mobile view