The following table lists the currently active PKCS standards.
Note: PKCS #2 and #4 do not exist anymore because they have been incorporated into PKCS #1.

Standard	Description
PKCS # 1	The RSA encryption standard. This standard defines mechanisms for encrypting and signing data using the RSA public key system.
PKCS # 3	The Diffie-Hellman key-agreement standard. This defines the Diffie-Hellman key agreement protocol.
PKCS # 5	The password-based encryption standard (PBE). This describes a method to generate a Secret Key based on a password.
PKCS # 6	The extended-certificate syntax standard. This is currently being phased out in favor of X509 v3.
PKCS # 7	The cryptographic message syntax standard. This defines a generic syntax for messages which have cryptography applied to it.
PKCS # 8	The private-key information syntax standard. This defines a method to store Private Key Information.

PKCS # 9 This defines selected attribute types for use in other PKCS standards.

PKCS # 10 The certification request syntax standard. This describes a syntax for certification requests.

PKCS # 11 The cryptographic token interface standard. This defines a technology independent programming interface for cryptographic devices such as smartcards.

PKCS # 12 The personal information exchange syntax standard. This describes a portable format for storage and transportation of user private keys, certificates etc.

PKCS # 13 The elliptic curve cryptography standard. This describes mechanisms to encrypt and sign data using elliptic curve cryptography.

PKCS # 14 This covers pseudo random number generation (PRNG). This is currently under active development.

PKCS # 15 The cryptographic token information format standard. This describes a standard for the format of cryptographic credentials stored on cryptographic tokens.