Standardy PKCS (Public-Key Cryptographic Standards)

Tyto standardy jsou dnes všeobecně známé a použité v celé řadě dnešních kryptografických produktů. Jedná se o de facto normy americké firmy RSA tzv. standardy PKCS (Public-Key Cryptographic Standards)

PKCS

Standardy PKCS jsou vytvářeny v laboratořích firmy RSA Security (dříve RSA) ve spolupráci s řadou vývojářů z celého světa. Poprvé tyto standardy byly publikovány v roce 1991 jako výsledek jednání určité skupiny pracovníků, kteří implementovali technologii kryptografie s veřejným klíčem (June 3 1991 , publikováno na : NIST/OSI Implementors' Workshop, dokument SEC-SIG-91-16.)

V roce 1993 bylo zveřejněno prvních deset standardů ve formální podobě, která je dodnes zachovávána.
Od té doby byly několikráte upravovány a doplňovány. Původní standardy PKCS #2 a PKCS #4 byly včleněny do PKCS #1 a tato čísla nejsou obsazena.

Dnes existují následující PKCS.

- **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**

Standard	PKCS #								External work
	1	3	5	6	7	8	9	10	
Algorithm-independent syntax:									
digitally signed messages					x		x		
digitally enveloped messages					x				
certification requests							x	x	
certificates									X.509, RFC 1422
extended certificates				x			x		
certificate-revocation lists									X.509, RFC 1422
encrypted private-key info.						x	x		
key agreement messages									[ISO90a], [ISO90b]
Algorithm-specific syntax:									
public keys: RSA	x								
private keys: RSA	x								
Algorithms:									
message digest: MD2, 5									RFCs 1319, 1321
secret-key encryption: DES									RFC 1423, [NIST92a]
public-key encryption: RSA	x								
signature: MD2, 4, 5 w/RSA	x								
password-based encryption			x						
key agreement: D-H		x							

[1] http://www.rsasecurity.com/rsalabs/pkcs/
[2] Burton S. Kaliski Jr. : An Overview of the PKCS Standards, An RSA Laboratories Technical Note
[3] Pro úvodní seznámení s obsahem standardů doporučuji seriál článků Jaroslava Pinkavy, který lze nalézt v e-zinech Crypto-World (http://crypto-world.info).
Kryptografie a normy I. (PKCS #1) , Crypto-World 9/2000
Kryptografie a normy II. (PKCS #3) Crypto-World 10/2000
Kryptografie a normy III. (PKCS #5) Crypto-World 11/2000
Kryptografie a normy IV. (PKCS #6, #7, #8) Crypto-World 12/2000
Kryptografie a normy V. (PKCS #9, 10, 11, 12, 15) Crypto-World 1/2001