haloooooooooo

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