Usage	Param Name	Param Val	Description	.NET	Windows native
JWS/JWE	alg/int	HS256	HMAC w/ SHA-256 hash	YES	XP SP2
JWS/JWE	alg/int	HS384	HMAC w/ SHA-384 hash	YES	XP SP2
JWS/JWE	alg/int	HS512	HMAC w/ SHA-512 hash	YES	XP SP2
JWS	alg	RS256	RSA w/ SHA-256 hash	YES	XP SP2
JWS	alg	RS384	RSA w/ SHA-384 hash	YES	XP SP2
JWS	alg	RS512	RSA w/ SHA-512 hash	YES	XP SP2
JWS	alg	ES256	ECDSA w/ P-256 curve and SHA-256 hash	YES	Vista
JWS	alg	ES384	ECDSA w/ P-384 curve and SHA-384 hash	YES	Vista
JWS	alg	ES512	ECDSA w/ P-521 curve and SHA-512 hash	YES	Vista
JWE	alg	RSA1_5	RSAES-PKCS1-V1_5	YES	XP SP2
JWE	alg	RSA-OAEP	RSAES OAEP	YES	XP SP2
JWE	alg	ECDH-ES	Elliptic Curve Diffie-Hellman Ephemeral Static	NO*	Vista
JWE	alg	A128KW	AES Key Wrap w/ 128 bit key	NO	Win7
JWE	alg	A256KW	AES Key Wrap w/ 256 bit key	NO	Win7
JWE	enc	A128CBC	AES CBC w/ 128 bit key	YES*	XP SP2
JWE	enc	A256CBC	AES CBC w/ 256 bit key	YES*	XP SP2
JWE	enc	A128GCM	AES GCM w/ 128 bit key	Codeplex	Vista SP1
JWE	enc	A256GCM	AES GCM w/ 256 bit key	Codeplex	Vista SP1
JWE	kdf	CS256	Concat Key Derivation Function (KDF)	NO	Win7
JWE	kdf	CS384	Concat Key Derivation Function (KDF)	NO	Win7
JWE	kdf	CS512	Concat Key Derivation Function (KDF)	NO	Win7

YES - Support built into library/platform
Release - Support included in this release of software and later
YES* - Supported but other non-supported code required (Concat KDF)
VARIES - In sources but often distributed w/ support compiled out
NO - Not supported in library/platform
NO* - Not supported in the specified configuration (w/ Concat KDF)
(blank) - Unknown
? - Answer is a first impression but requires more research

PHP version 5.2
PHPSecLib version 0.3.0
PyCrypto version 2.6
Ruby 1.9.3 with ruby-openssl
Java 7
OS X 10.6 (Snow Leopard)

OS X	iOS	Java JCA	BouncyCastle	Android	PHP	PHPSecLib	Python	M2Crypto	PyCrypto	Ruby
YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
YES	YES	YES	YES	YES	NO	YES	NO	YES	YES	YES
YES	YES	YES	YES	YES	NO	YES	NO	YES	YES	YES
YES	YES	YES	YES	YES	NO	YES	NO	YES	YES	YES
10.6	NO	YES?	YES	YES	NO	NO	NO	YES	NO	YES
10.6	NO	YES?	YES	YES	NO	NO	NO	YES	NO	YES
10.6	NO	YES?	YES	YES	NO	NO	NO	YES	NO	YES
YES	YES	YES	YES	YES	YES	YES	NO	YES	YES	
YES?	YES	YES	YES	YES	NO	YES	NO	YES	YES	
NO?	NO	YES*	YES*	YES*	NO	NO	NO	YES?	NO	
YES	YES		YES	YES	NO	NO	NO	YES	YES	
YES	YES		YES	YES	NO	NO	NO	YES	YES	
YES		YES*	YES*	YES*	YES*	YES*	NO	YES*	YES*	
YES		YES*	YES*	YES*	YES*	YES*	NO	YES*	YES*	
NO?	NO	NO	YES	YES	NO	NO	NO	NO?	NO	
NO?	NO	NO	YES	YES	NO	NO	NO	NO?	NO	
		NO	NO	NO	NO	NO	NO	NO	NO	
		NO	NO	NO	NO	NO	NO	NO	NO	
		NO	NO	NO	NO	NO	NO	NO	NO	

BouncyCastle is a crypto lib for Java

Android uses BouncyCastle

PHPSecLib is a crypto lib for PHP

M2Crypto is a crypto lib for Python

PyCrypto is a crypto lib for Pyth

NSS is the crypto lib

OpenSSL	node.js	NSS
YES	YES	YES
YES	YES	YES
YES	YES	YES
YES	YES	YES
YES	YES	YES
YES	YES	YES
VARIES	VARIES?	VARIES
VARIES	VARIES?	VARIES
VARIES	VARIES?	VARIES
YES	YES	YES
YES	YES	NO
VARIES?	VARIES?	NO?
YES?	YES?	NO
YES?	YES?	NO
YES*	YES*	YES*
YES*	YES*	YES*
YES	YES	NO
YES	YES	NO
NO	NO	NO
NO	NO	NO
NO	NO	NO

on
used by Firefox