Key Exchange Algorithm	**Required Certificate Type**	**ServerKeyExchange required?**	**Content ClientKeyExchange**	**Description**
RSA	RSA Encryption	No	Encrypted PremasterSecret	Client encrypts PremasterSecret with the public key of the server.
RSA Export	RSA Signing	Yes (temporary RSA key $\leq$ 512 bit)	With temp. RSA key encrypted PremasterSecret	Client encrypts PremasterSecret with temporary RSA Key of the server (only relevant for backward compatibility).
DHE-DSS	DSS Signing	Yes (g^s mod p)	g^c mod p	Diffie-Hellman key agreement, server signed g^s mod p with the DSS - key.
DHE-RSA	RSA Signing	Yes (g^s mod p)	g^c mod p	Diffie-Hellman key agreement, server signed g^s mod p with the RSA key.
DH-DSS	DH, signed with DSS	No (g^s mod p included in the certificate)	g^c mod p	Diffie-Hellman key agreement with fixed server share, authentication via DSS certificate
DH-RSA	DH, signed with RSA	No (g^c mod p included in certificate)	g^c mod p	Diffie-Hellman key agreement with fixed server share, authentication via RSA certificate