COSE_Recipient Types

Alg ID	Name	Method class in RFC 9052	Method definition	Uses KDF & CIS	Protects headers	Vulnerable to AEAD downgrade	COSE_Recipient contents
-3	A128KW	8.5.2. Key Wrap	RFC 9053 6.2.1. AES Key Wrap	No	No	Yes	Ciphertext is wrapped key
-4	A192KW						
-5	A256KW						
-6	Direct	8.5.1. Direct Encryption	RFC 9053 6.1.1. Direct Key	No	No	Yes	Kid parameter. Probably just use Encrypt0 instead of this.
-10	direct+HKDF-SHA-256	8.5.1. Direct Encryption	RFC 9053 6.1.2. Direct Key with KDF	Yes	Yes	No	Salt or partyU parameter required. No ciphertext.
-11	direct+HKDF-SHA-512						
-12	direct+HKDF-AES-128						
-13	direct+HKDF-AES-256						
-25	ECDH-ES + HKDF-256	8.5.4. Direct Key Agreement	RFC 9053 6.3.1. Direct ECDH	Yes	Yes	No	ephemeral_key parameter. No ciphertext.
-26	ECDH-ES + HKDF-512						
-27	ECDH-SS + HKDF-256						
-28	ECDH-SS + HKDF-512						
-29	ECDH-ES + A128KW	8.5.5. Key Agreement with Key Wrap	RFC 9053 6.4.1. ECDH with Key Wrap	Yes	Yes	Yes	ephemeral_key parameter. ciphertext is wrapped key
-30	ECDH-ES + A192KW						
-31	ECDH-ES + A256KW						
-32	ECDH-SS + A128KW						
-33	ECDH-SS + A192KW						
-34	ECDH-SS + A256KW						
-40	RSAES-OAEP w/ RFC 8017 default parameters	8.5.3. Key Transport	RFC 8230 3 RSA-ES-OAEP	No	No	Yes	Ciphertext is the encrypted key
-41	RSAES-OAEP w/ SHA-256						
-42	RSAES-OAEP w/ SHA-512						