IANA COSE Registrations

COSE WG, February 17, 2021

Purpose

- Discussion of IANA COSE registrations
  - Algorithms, Elliptic Curves
  - https://mailarchive.ietf.org/arch/msg/cose/JQG38ywtoQvKe1bgDm2Ajk5e9Nk/

- Purpose of these slides: Summarize discussion and progress open points.

Algorithm not bundled with curve

- Signature algorithm is bundled with a hash function but not with the elliptic curve.
- Section 2.1 of RFC 8152

  "This document defines ECDSA to work only with the curves P-256, P-384, and P-521. Future documents may define it to work with other curves and points in the future."
- Agree that ES256K is an exception
  - to restrict the use in COSE to the legacy case compatibile with existing signing hardware
  - the limit the risk due to misinterpreting secp256k1 points with secp256r1 points

- Similarly, ECDH is bundled with key derivation/wrap but not with the elliptic curve.
- Agree that new registrations should follow the rule not the exception
  - If new property of algorithm, it should be defined generally rather than for a specific curve only

ES256K	-47	ECDSA using secp256k1, SHA-256

EdDSA	-8	EdDSA (with SHA-512)
ES256	-7	ECDSA w/ SHA-256

Cofactor different from 1

- RFC 8152 (referring to RFC 6090) assume EC groups of cofactor = 1
- For cofactor != 1 multiply by cofactor in ECDH to protect against attacks with small subgroups
- Do we need to register new ECDH algorithms for cofactor != 1?

Candidate solutions:

1. For each ECDH algorithm, define one with cofactor != 1
   - Duplicates all ECDH registrations
2. Clear the cofactor multiplication in the ECDH operation/shared secret encoding.
   - Define in the curve specification (not defined in RFC 8152)

Solution 2. seems more robust

- no way to perform non-cofactor ECDH with this curv
- With solution 1 implementer may accidently use cofactor=1 code point and ECDH/shared secret calculation

		256-bit key			
ECDH-ES + A192KW	-30	ECDH ES w/ Concat KDF and AES Key Wrap w/ 192-bit key	[kty]	[RFC-ietf-cose-rfc8152bis-algs-12]	Yes
ECDH-ES + A128KW	-29	ECDH ES w/ Concat KDF and AES Key Wrap w/ 128-bit key	[kty]	[RFC-ietf-cose-rfc8152bis-algs-12]	Yes
ECDH-SS + HKDF-512	-28	ECDH SS w/ HKDF - generate key directly	[kty]	[RFC-ietf-cose-rfc8152bis-algs-12]	Yes
ECDH-SS + HKDF-256	-27	ECDH SS w/ HKDF - generate key directly	[kty]	[RFC-ietf-cose-rfc8152bis-algs-12]	Yes
ECDH-ES + HKDF-512	-26	ECDH ES w/ HKDF - generate key directly	[kty]	[RFC-ietf-cose-rfc8152bis-algs-12]	Yes
ECDH-ES + HKDF-256	-25	ECDH ES w/ HKDF - generate key directly	[kty]	[RFC-ietf-cose-rfc8152bis-algs-12]	Yes

Deterministic signatures

- Deterministic ECDSA is recommended
- Agree that specifications can use ECDSA code point without using deterministic signature

(We should probably change this recommendation – separate issue.)

ECDSA with SHAKE-256

- Request to register a curve for use with ECDSA and SHAKE-256

- Would need to register ECDSA with SHAKE-256
- Similar to ecdsa-with-shake256 in RFC 8692

Multiple key types

- Request to specify a curve with both EC2 and OKP
- Current registration has only one key type per curve
- RFC 8152 and its successor define ECDSA to only work with EC2
  - Unclear if future specifications can deviate from this or not
  - RFC 8152 only mentions new curves may be defined

[Not clear to me why OKP is needed]

P-256	1	EC2	NIST P-256 also known as secp256r1		[RFC-ietf-cose-rfc8152bis-algs-12]	Yes
P-384	2	EC2	NIST P-384 also known as secp384r1		[RFC-ietf-cose-rfc8152bis-algs-12]	Yes
P-521	3	EC2	NIST P-521 also known as secp521r1		[RFC-ietf-cose-rfc8152bis-algs-12]	Yes
X25519	4	OKP	X25519 for use w/ ECDH only		[RFC-ietf-cose-rfc8152bis-algs-12]	Yes
X448	5	OKP	X448 for use w/ ECDH only		[RFC-ietf-cose-rfc8152bis-algs-12]	Yes
Ed25519	6	OKP	Ed25519 for use w/ EdDSA only		[RFC-ietf-cose-rfc8152bis-algs-12]	Yes
Ed448	7	OKP	Ed448 for use w/ EdDSA only		[RFC-ietf-cose-rfc8152bis-algs-12]	Yes
secp256k1	8	EC2	SECG secp256k1 curve	IESG	[RFC8812]	No

EC code point values

— Informational RFC cannot register the shortest values

Range	**Registration Procedures**
Integer values -65536 to -257	Specification Required
Integer values -256 to 255	Standards Action With Expert Review
Integer values 256 to 65535	Specification Required
Integer values greater than 65535	Expert Review