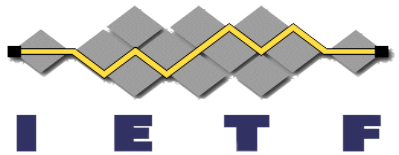
Fully-Specified Algorithms for JOSE and COSE



draft-ietf-jose-fully-specified-algorithms

Mike Jones and Orie Steele
IETF 120, Vancouver
July 22, 2024

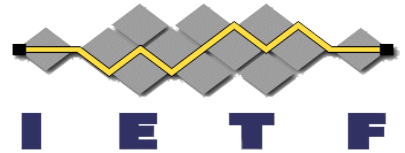
Why and What

- See Introduction in draft-ietf-jose-fully-specified-algorithms
- Or IETF 118 slides https://datatracker.ietf.org/meeting/118/materials/slides-118-jose-fully-specified-algorithms-for-jose-and-cose-00

Progress Since IETF 119

- At IETF 119 in Brisbane, described current working group draft
  - And remaining open issue on fully-specified ECDH encryption algorithms
- Held “Fully-specified ECDH algorithms” list discussion in April
- Working Group Last Call (WGLC) on -02 in May
  - Actionable, constructive feedback received
- Published -03 incorporating WGLC feedback in July

Draft -03 Addressing WGLC Feedback



- Acknowledged contributions made during WGLC
- Addressed security considerations feedback from WGLC
- Made COSE Recommended status for Ed25519 and Ed448 "yes"
- Registered COSE algorithms using Brainpool curves with ECDSA
- Removed text on KEMs, since currently registered algorithms don't use them
- Enabled use of fully-specified ECDH algorithms
- Defined the terms "Deprecated" and "Prohibited" for both JOSE and COSE registrations

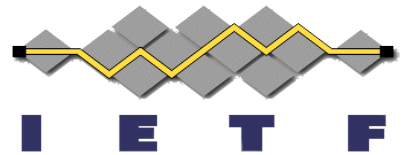
Made COSE Recommended status for Ed25519 and Ed448 "yes"

Name	COSE Value	Description	JOSE Implementation Requirements	COSE Recommended
Ed25519	TBD (requested assignment -50)	EdDSA using Ed25519 curve	Optional	Yes
Ed448	TBD (requested assignment -51)	EdDSA using Ed448 curve	Optional	Yes

Registered COSE algorithms using Brainpool curves with ECDSA

Name	COSE Value	Description	COSE Recommended
ESB256	TBD (requested assignment -261)	ECDSA using BrainpoolP256r1 curve and SHA-256	No
ESB320	TBD (requested assignment -262)	ECDSA using BrainpoolP320r1 curve and SHA-384	No
ESB384	TBD (requested assignment -263)	ECDSA using BrainpoolP384r1 curve and SHA-384	No
ESB512	TBD (requested assignment -264)	ECDSA using BrainpoolP512r1 curve and SHA-512	No

Enabled use of fully-specified ECDH algorithms



- Created appendix “Inventory of Polymorphic ECDH Algorithms”
  - Inventories registered polymorphic JOSE and COSE ECDH algorithms
  - Describes fully-specified variants of all these algorithms
- Creates small set of fully-specified ECDH algorithms
  - 2 for JOSE, 4 for COSE
  - Use P-256 and sometimes A128KW
  - Enabling use of ECDH with only fully-specified algorithms
  - Provides example for future specs that could register more, when needed
- Compromise based on WG feedback
  - Do something since the problem is real, but don’t do everything right now

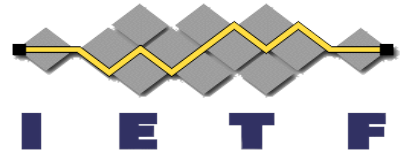
Fully-Specified JOSE ECDH Algs

Name	Description	Implementation Requirements
ECDH-ES-P-256	ECDH-ES using Concat KDF and P-256	Recommended
ECDH-ES-P-256+A128KW	ECDH-ES using Concat KDF and P-256 and "A128KW" wrapping	Recommended

Fully-Specified COSE ECDH Algs

Name	COSE Value	Description	Recommended
ECDH-ES-P-256 + HKDF-256	TBD (requested assignment -52)	ECDH ES using P-256 w/ HKDF -- generate key directly	Yes
ECDH-SS-P-256 + HKDF-256	TBD (requested assignment -53)	ECDH-SS using P-256 w/ HKDF -- generate key directly	Yes
ECDH-ES-P-256 + HKDF-256 + A128KW	TBD (requested assignment -54)	ECDH ES using P-256 w/ HKDF and AES Key Wrap w/ 128-bit key	Yes
ECDH-SS-P-256 + HKDF-256 + A128KW	TBD (requested assignment -55)	ECDH-SS using P-256 w/ HKDF and AES Key Wrap w/ 128-bit key	Yes

Defined terms "Deprecated" and "Prohibited" for both registrations



- Use of these terms between JOSE & COSE currently inconsistent
- Spec consistently defines these terms for use by both
  - **Deprecated** – There is a preferred mechanism to achieve similar functionality to that referenced by the identifier; this replacement functionality SHOULD be utilized in new deployments in preference to the deprecated identifier.
  - **Prohibited** – The identifier and the functionality that it references MUST NOT be used. (Identifiers MAY be designated as "Prohibited" due to security flaws, for instance.)
- Consistent with existent registrations for both JOSE and COSE
  - None will have to change

Status

- Draft -03 solves the existing problems we're chartered to address
- Tradeoffs incorporated based on extensive WG feedback (thanks!)
  - Solves the problems now that people identified as immediate pain points
  - Documents how future specs can solve additional problems when they are identified as pain points
- Prevents the problems from getting worse
- Authors appreciate the vigorous working group engagement
  - Substantially improved the specification!

Next Steps

- Second working group last call?