Fully-Specified Algorithms for JOSE and COSE

draft-jones-jose-fully-specified-algorithms

Mike Jones and Orie Steele
IETF 118, Prague
November 10, 2023
Progress Since IETF 117

- At IETF 117 in San Francisco, Orie Steele and I proposed a spec defining fully-specified algorithms for JOSE and COSE
  - Positive feedback and concrete suggestions received there
- Wrote draft-jones-jose-fully-specified-algorithms incorporating the feedback
  - -00 published in August
  - -01 published soon thereafter, renaming some things by acclamation!
  - -02 published in October, addressing many of the to-do items
Why and What

- Next few slides recap motivations and approach
Fully-Specified vs. Polymorphic Algorithms

The IANA algorithm registries for JOSE and COSE contain two kinds of algorithm identifiers:

- **Fully-Specified** – Those that fully determine the cryptographic operations to be performed
  - Including any Curve, KDF, Hash Function, etc.
  - Examples: RS256, ES256K, ES256 (in JOSE)

- **Polymorphic** – Those requiring info beyond the identifier to determine the cryptographic operations to be performed
  - Such as the cryptographic key with a curve
  - Examples: EdDSA, ES256 (in COSE)
Why It Matters

Many protocols negotiate supported operations using just “alg”

- RFC 8414 (AS Metadata) uses negotiation parameters like:
  "token_endpoint_auth_signing_alg_values_supported": ["RS256", "ES256"]
- OpenID Connect negotiates using “alg” and “enc” values
- WebAuthn and FIDO2 negotiate using COSE “alg” numbers

This doesn’t work for polymorphic algorithms:

- With “EdDSA”, you don’t know which of Ed25519 or Ed448 are supported!
- WebAuthn contains this definition as a result:
  - “-8 (EdDSA), where crv is 6 (Ed25519)”
Spec registers fully-specified algorithm values for these algorithms currently using polymorphic values:

- “Ed25519” – Edwards-curve Digital Signature with Ed25519 curve (for both)
- “Ed448” – Edwards-curve Digital Signature with Ed448 curve (for both)
- “ESP256” – ECDSA using P-256 curve and SHA-256 (for COSE)
- “ESP384” – ECDSA using P-384 curve and SHA-384 (for COSE)
- “ESP512” – ECDSA using P-521 curve and SHA-512 (for COSE)
Updating Polymorphic RFCs

- The spec adds “Updated by” to existing RFCs registering polymorphic algorithm identifiers
  - RFC 8037: CFRG Elliptic Curve Diffie-Hellman (ECDH) and Signatures in JSON Object Signing and Encryption (JOSE)
  - RFC 9053: CBOR Object Signing and Encryption (COSE): Initial Algorithms
- Gives implementers notice of fully-specified algorithms
Updating Designated Expert Instructions

- The spec proposes updated instructions to the designated experts for the JOSE and COSE algorithm registries established by:
  - RFC 7518: JSON Web Algorithms (JWA)
  - RFC 9053: CBOR Object Signing and Encryption (COSE): Initial Algorithms
- Would instruct the experts not to approve any more polymorphic algorithm identifier registrations
- This would prevent the problem from getting worse
Next Steps

- Time for working group adoption?
BACKUP SLIDES
Should it be a BCP?

- Should this specification be a Best Current Practices document?
- It would make using fully-specified algorithm identifiers a Best Current Practice