*

# Fully-Specified Algorithms for JOSE and COSE

***draft-ietf-jose-fully-specified-algorithms***

Mike Jones – Self-Issued Consulting
OAuth Security Workshop – Rome
April 12, 2024

# 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)"

# New Fully-Specified Algorithms

| Identifier | Description |
|---|---|
| Ed25519 | Edwards-curve Digital Signature with Ed25519 curve (for both JOSE and COSE) |
| Ed448 | Edwards-curve Digital Signature with Ed448 curve (for both JOSE and COSE) |
| ESP256 | ECDSA using P-256 curve and SHA-256 (only needed for COSE) |
| ESP384 | ECDSA using P-384 curve and SHA-384 (only needed for COSE) |
| ESP512 | ECDSA using P-521 curve and SHA-512 (only needed 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

# Updates Designated Expert Instructions

- The spec updates 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
- Instructs the experts not to approve any more polymorphic algorithm identifier registrations
- This will prevent the problem from getting worse

# Open Question on ECDH

- ECDH-ES, ECDH-ES+A128KW, etc. take ephemeral key as a parameter
  - Meaning that they are polymorphic
- Should we create fully-specified algorithm identifiers?
  - Such as ECDH-ES-ES256, ECDH-ES-ES256+A128KW, etc.
- Some on the list are saying that we should do the whole job
- Others advocating only registering fully-specified ECDH algorithm identifiers when there's a demonstrated needed for them
- Asked question to jose@ietf.org this week

# Current JOSE ECDH Algorithms

| Identifier | Description |
|---|---|
| ECDH-ES | ECDH-ES using Concat KDF |
| ECDH-ES+A128KW | ECDH-ES using Concat KDF and "A128KW" wrapping |
| ECDH-ES+A192KW | ECDH-ES using Concat KDF and "A192KW" wrapping |
| ECDH-ES+A256KW | ECDH-ES using Concat KDF and "A256KW" wrapping |

# Possible Fully-Specified JOSE ECDH Algorithms

| Identifier | Description |
|---|---|
| ECDH-ES-P-256 | ECDH-ES using Concat KDF and P-256 |
| ECDH-ES-P-384 | ECDH-ES using Concat KDF and P-384 |
| ECDH-ES-P-521 | ECDH-ES using Concat KDF and P-521 |
| ECDH-ES-X25519 | ECDH-ES using Concat KDF and X25519 |
| ECDH-ES-X448 | ECDH-ES using Concat KDF and X448 |
| ECDH-ES-P-256+A128KW | ECDH-ES using Concat KDF and P-256 and "A128KW" wrapping |
| ECDH-ES-X25519+A128KW | ECDH-ES using Concat KDF and X25519 and "A128KW" wrapping |
| ECDH-ES-P-384+A192KW | ECDH-ES using Concat KDF and P-384 and "A192KW" wrapping |
| ECDH-ES-P-521+A256KW | ECDH-ES using Concat KDF and P-521 and "A256KW" wrapping |
| ECDH-ES-X448+A256KW | ECDH-ES using Concat KDF and X448 and "A256KW" wrapping |

# Equivalent ECDH Analysis for COSE

- Available in my message to jose@ietf.org
- 10 registered polymorphic COSE ECDH algorithms
  - Both ECDH-ES and ECDH-SS variants
- Would be replaced by 18 fully-specified COSE ECDH algorithms

# Observations

- This work is already having the intended effect
- New algs being developed for JOSE and COSE are fully-specified
  - HPKE algorithms
  - Post-quantum algorithms

# Next Steps

- Resolve ECDH question
  - Update the draft accordingly
- Then likely working group last call

- Let’s discuss!