PQ/T Hybrid Composite Signatures for JOSE and COSE

draft-prabel-jose-pq-composite-sigs-00

Lucas PRABEL, Shuzhou SUN

IETF 121, Dublin

PQ/T Composite Signatures

PQ/T Hybrid Digital Signature *Definition from* draft-ietf-pquip-pqt-hybrid-terminology

A multi-algorithm digital signature scheme made up of two or more **component** digital signature algorithms where at least one is a **post-quantum algorithm** and at least one is a **traditional algorithm**.

PQ/T Hybrid Composite Digital Signature *Definition from* draft-ietf-pquip-pqt-hybrid-terminology

A PQ/T Hybrid Digital Signature where and the resulting composite scheme is exposed as a **singular interface** of the same type as the component algorithms.

→ approach used for X.509, PKIX, CMS in draft-ietf-lamps-pq-composite-sigs

JOSE & COSE algorithms using ML-DSA with ECDSA

JOSE Composite Signature Algorithms for ML-DSA

Name	First Algorithm	Second Algorithm	Pre-Hash	Description
MLDSA44-ES256	ML-DSA-44	ecdsa-with-SHA256 with secp256r1	id-sha256	Composite Signature with ML-DSA-44 and ECDSA using P-256 curve and SHA-256
MLDSA65-ES512	ML-DSA-65	ecdsa-with-SHA512 with secp256r1	id-sha512	Composite Signature with ML-DSA-65 and ECDSA using P-256 curve and SHA-512
MLDSA87-ES512	ML-DSA-87	ecdsa-with-SHA512 with secp384r1	id-sha512	Composite Signature with ML-DSA-87 and ECDSA using P-384 curve and SHA-512

COSE Composite Signature Algorithms for ML-DSA

Name	COSE Value	First Algorithm	Second Algorithm	Pre-Hash	Description
MLDSA44-ES256	TBD (request assignment -51)	ML-DSA-44	ecdsa-with-SHA256 with secp256r1	id-sha256	Composite Signature with ML-DSA-44 and ECDSA using P-256 curve and SHA-256
MLDSA65-ES512	TBD (request assignment -52)	ML-DSA-65	ecdsa-with-SHA512 with secp256r1	id-sha512	Composite Signature with ML-DSA-65 and ECDSA using P-256 curve and SHA-512
MLDSA87-ES512	TBD (request assignment -53)	ML-DSA-87	ecdsa-with-SHA512 with secp384r1	id-sha512	Composite Signature with ML-DSA-87 and ECDSA using P-384 curve and SHA-512

Composite Keys & Signature Structures

```
(pk_1, sk_1) <- MLDSA.KeyGen()
(pk_2 = (x,y), sk_2 = d) <- ECDSA.KeyGen()

Composite Public Key <- pk_1 || pk_2 = pk_1 || x || y
Composite Private Key <- sk_1 || sk_2 = sk_1 || d
```

```
M' <- Domain || HASH(M)
M' <- Encode(M')

sig_1 <- MLDSA.Sign(sk_1, M')
sig_2 <- ECDSA.Sign(sk_2, M')

Composite Signature <- (sig_1, sig_2)
```

Domain Separator for JOSE/COSE

Domain = octets of the ASCII representation of the Composite Signature "alg" (algorithm) Header Parameter value.

ML-DSA Private Key Format

ML-DSA Private key are stored as a **32-byte seed.**

JOSE & COSE Composite Signature Key Types & Parameters

JWK Key Type for Composite algorithms

kty	Description
AKP-EC	JWK key type for composite signature with ECDSA as the traditional component.

COSE Key Type for Composite algorithms

Name	kty	Description
AKP-EC2	TBD	COSE key type for composite algorithm with ECDSA as the traditional component.

"AKP" Key Type chosen in order to align with draft-ietf-cose-dilithium

JSON AKP-EC Web Key Parameters

Parameter Name	Parameter Description	Used with "kty" Value(s)	Parameter Information Class	Change Controller	Specification Document(s)
pub	Public Key	AKP-EC	Public	IETF	n\a
priv	Private Key	AKP-EC	Private	IETF	n\a

+ **crv, x, y, d** used with "kty" value **AKP-EC**

COSE AKP-EC2 Key Parameters

Key Type	Name	Label	CBOR Type	Description
TBD (request assignment 8)	crv	-1	int / tstr	EC identifier
TBD (request assignment 8)	x	-2	bstr	x-coordinate
TBD (request assignment 8)	y	-3	bstr / bool	y-coordinate
TBD (request assignment 8)	d	-4	bstr	EC Private key
TBD (request assignment 8)	pub	-5	bstr	Public Key
TBD (request assignment 8)	priv	-6	bstr	Private Key

Next Steps

- **Composite algorithms:** which one to register?
- **ML-DSA Private Keys:** Seed or Full expanded key?
- **Domain Seprator:** what is the best definition?
- **Pre-hash Option?**

Comments and suggestions are welcome

Thank You

draft-prabel-jose-pq-composite-sigs-00