

Cryptographic suites

Separate reference formation, identity proof and protected-channel construction.

01 Three independent choices

REFERENCE
Hash + identifier length

IDENTITY PROOF
Signing identity + proof

CHANNEL
Key establishment + protection

A post-quantum signature does not make a classical key exchange post-quantum.

02 Identity suites / reference-suite registry

ID	Signature	Reference hash	ID bytes	Public key	Proof bytes
0x0001	Ed25519(BLAKE3)	BLAKE3	32	32	64
0x0002	Ed25519ctx	SHA-256	32	32	64
0x0003	ML-DSA-65	SHA-256	32	1952	3309
0x0004	ML-DSA-87	SHA-384	48	2592	4627
0x0005	Ed25519(BLAKE3) + ML-DSA-87	BLAKE3	32	2624	4691

SCIR envelope: header[1] + reference_suite[2] + identifier[L]. Current L: 32 or 48 octets.
For ALIAS / MULTICAST / GROUPOCAST, the reference suite does not select the external signer.

03 Session-suite registry / version 4 inventory

ID	Key establishment	Record protection	Key derivation	Transcript
0x0001	NONE	NONE	—	BLAKE3
0x0002	NONE	NONE	—	SHA-256
0x0101	X25519	ChaCha20-Poly1305	BLAKE3 derive-key	BLAKE3
0x0102	X25519	AES-256-GCM	BLAKE3 derive-key	BLAKE3
0x0201	X25519 + ML-KEM-768	ChaCha20-Poly1305	BLAKE3 derive-key	BLAKE3
0x0202	X25519 + ML-KEM-1024	ChaCha20-Poly1305	BLAKE3 derive-key	BLAKE3
0x0301	ML-KEM-768	AES-256-GCM	HKDF / SHA-256	SHA-256
0x0302	ML-KEM-1024	AES-256-GCM	HKDF / SHA-384	SHA-384

0101–0102: classical · 0201–0202: hybrid · 0301–0302: post-quantum key establishment.
NONE has no encryption or AEAD tag. Protected rows: nonce 12 octets, tag 16 octets.

04 Selected HS2 laboratory profiles / A1 · B1 · C1

A1: identity suite 0x0002; Ristretto-based construction, BLAKE3 derivation, ChaCha20-Poly1305.
B1/C1: Ristretto255 + HKDF/HMAC-SHA-256 + ChaCha20-Poly1305; B1 adds Ed25519ctx.
C1 proves no identity. These profiles do not enable the full v4 inventory or select NONE.

READ IDS WITH THEIR REGISTRY

Identity 0x0002 and session 0x0002 mean different things. Registry presence is not profile support.