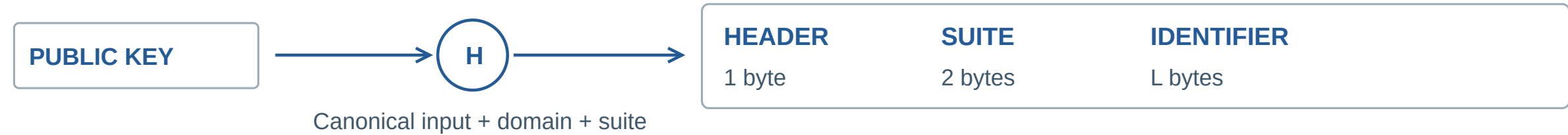


Cryptography

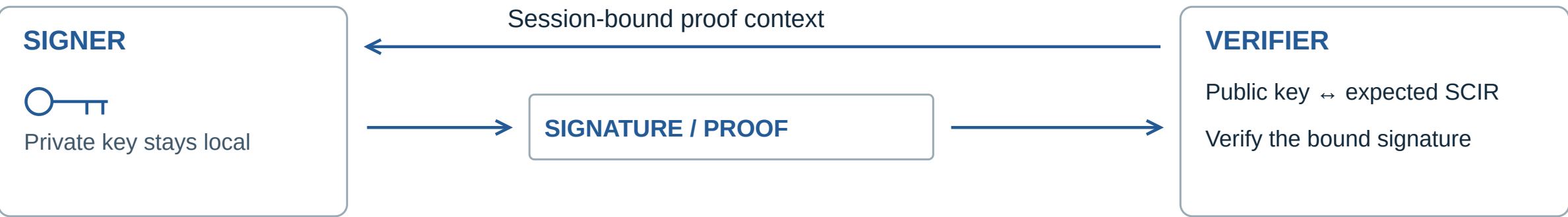
Follow the operations: reference → proof → shared keys → protected records.

01 Form a reference



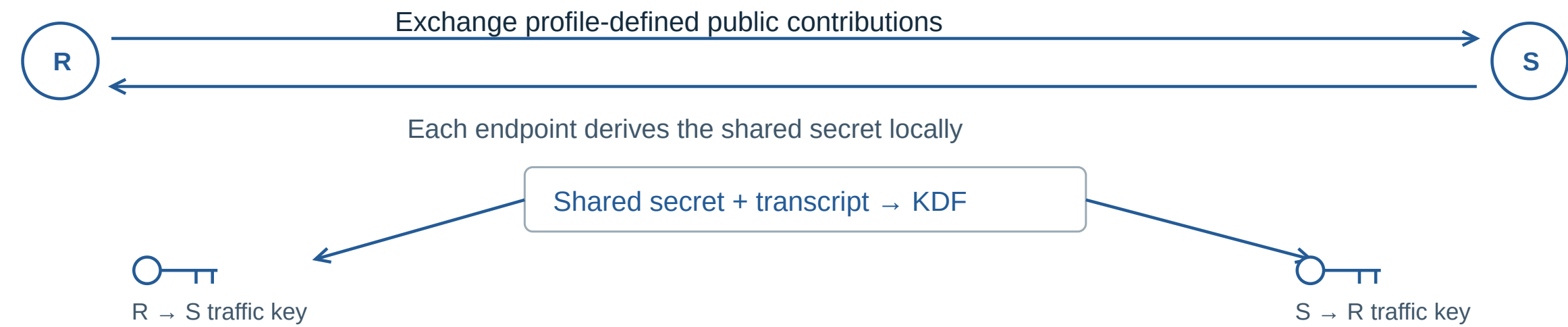
An IDENTITY SCIR commits to public-key material. Its identifier length is defined by the suite.

02 Prove control of the referenced key



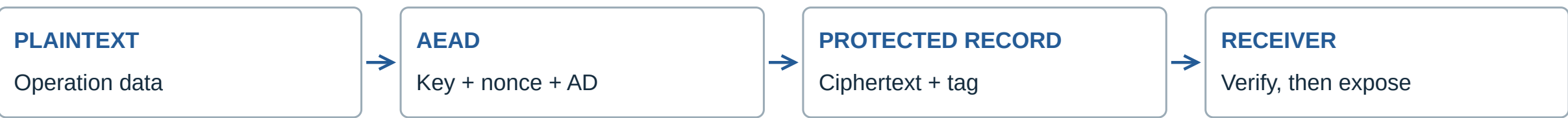
Valid proof establishes key control. Service policy separately decides permission.

03 Establish and derive channel keys



V4 choices: X25519 (classical) · ML-KEM (post-quantum) · X25519 + ML-KEM (hybrid).

04 Protect and verify each record



AD = authenticated associated data. Nonces must not repeat under the same key.

Receiver acceptance also checks current authority, sequence and replay state.

05 Selected HS2 laboratory profiles

A1

Ed25519ctx identity proof
Ristretto-based establishment
BLAKE3 → ChaCha20-Poly1305

B1

Ed25519ctx identity proof
Ristretto255 establishment
HKDF/HMAC → ChaCha20-Poly1305

C1

No identity proof
Ristretto255 establishment
HKDF/HMAC → ChaCha20-Poly1305

COMPANION / CRYPTOGRAPHIC SUITES

Full IDs, algorithms and lengths are in the reference sheet. Signature and key-exchange choices are distinct.