Handshake Message Sequence (Transcript-Bound)

Initiator

Responder

MessageA
version, supportedSuites[], policy, keyShares[], nonces
sigA, identityPubKey, seSigA (opt)

MessageB
selectedSuite, responderShare, nonce, encrypted payload
sigB, identityPubKey, seSigB (opt)

Finished_R2I
HMAC(finishedKey_R, transcriptHash)

Finished_I2R
HMAC(finishedKey_I, transcriptHash)

Transcript Hash Coverage

MessageA || MessageB || Finished_R2I || Finished_I2R

Policy is wire-visible and auditable (in MessageA)