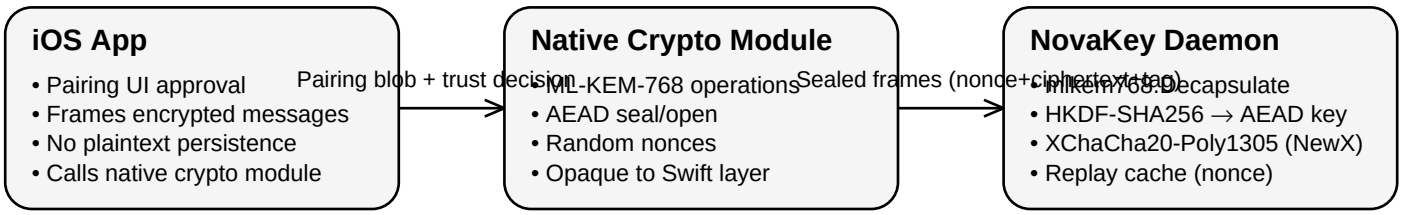
# NovaKey Crypto Architecture (Daemon-Anchored)

ML-KEM-768 (Kyber768) • HKDF-SHA256 • XChaCha20-Poly1305 • Replay Protection




## Daemon-Anchored Protocol Flow

1) Pairing: Daemon receives Kyber ciphertext; decapsulates via mlkem768.Decapsulate (pairing_proto.go:145) to obtain sharedKem.
2) KDF: Daemon derives AEAD key using HKDF-SHA256 with context string "NovaKey v3 AEAD key" (crypto.go:153–156).
3) AEAD: Daemon constructs XChaCha20-Poly1305 via NewX (crypto.go:254) and parses nonce+ciphertext (crypto.go:260–266).
4) Verify: AEAD.Open authenticates header+Aead payload (crypto.go:268). Tamper causes failure.
5) Replay: Nonce checked against per-device replay cache (crypto.go:56, 323–328); reuse is rejected.
6) Gating: Decrypted plaintext passes policy and two-man gates before injection (msg_handler.go:69–200).

## Security Properties (Daemon-Enforced)

• Confidentiality + integrity in transit (XChaCha20-Poly1305 AEAD).
• Post-quantum session establishment (ML-KEM-768 / Kyber768).
• Forward secrecy at session level (fresh sharedKem per pairing/session).
• Strong replay protection (nonce cache per deviceID).
• No cloud key escrow; all keys remain local.