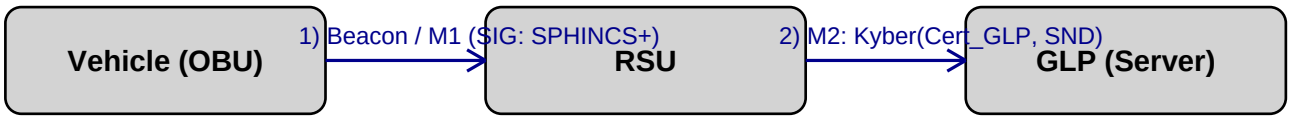
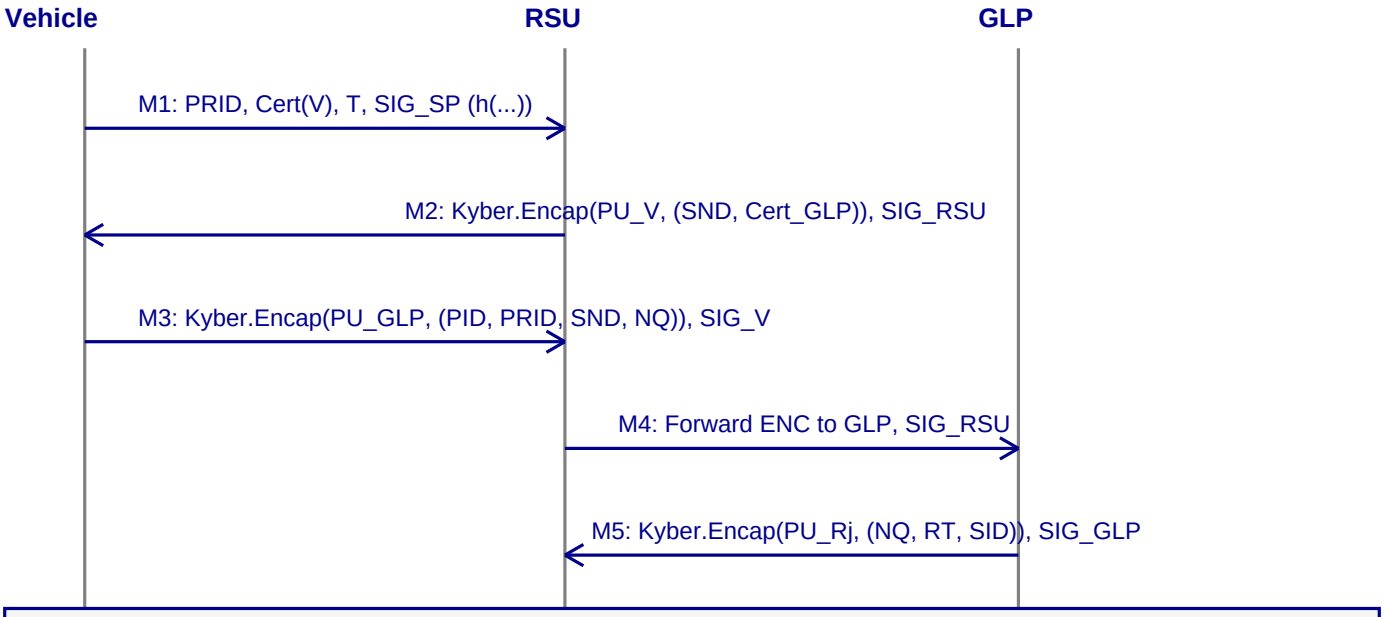
Quantum-Resilient IoV Protocol — Improved Flowmaps

Hybrid design: SPHINCS+ (signatures) + CRYSTALS-Kyber (KEM). Optimized for low latency.





Notes and Performance (practical estimates):

- SPHINCS+-128s signature: ~7.8 KB, sign time ~1–10 ms (device dep.).
- Kyber-768 ciphertext: ~1.1 KB; encaps/decaps << 1 ms on modern CPUs.
- Use hybrid (classical + PQ) for transitional compatibility; keep heavy signs limited.

Primitive	PubKey	Sig / Ciphertext	Typical CPU cost
ECDSA-P256	32 B	64 B sig	Very fast
SPHINCS+-128s	32 B	≈7.8 KB sig	Slower (ms)
CRYSTALS-Kyber-768	≈1.1 KB	≈1.1 KB ct	Very fast (<1 ms)