

Post-Quantum Authentication in Carrier Networks: BGPsec/RPKI, SRv6 and Agentic AI NetOps

Jaypal Baviskar · Afshan Mulla

Technical Leader, Cisco CX (views our own)

IAB Workshop on Accelerating the Deployment of Post-Quantum Authentication (pqws) · Prague, 11–12 October 2026

Signatures are the harder half of the quantum transition

Symmetric crypto survives; key agreement is migrating; signatures are big and must last

✓ Survives

AES, SHA-2/3, HMAC

Grover only halves strength

3,309 B

ML-DSA-65 signature

✗ Breaks

RSA / ECDH key agreement

→ ML-KEM (FIPS 203), already migrating

~13x

vs RSA-2048 (RPKI today)

✗ Breaks

RSA / ECDSA signatures

→ ML-DSA (FIPS 204), SLH-DSA (FIPS 205): the harder half

~47x

vs ECDSA P-256 (BGPsec)

The real risk: signatures have no harvest-now-decrypt-later problem. The risk is anything that must still be trusted after a quantum computer arrives: trust anchors, long-lived certificates, audit records. Nothing is broken today; this is a migration problem.

Carrier Networks: Same pressure, three different walls

PQ signatures are big and must last; each carrier surface fails differently

1 RPKI / BGPsec

Too many signatures

RPKI signs every certificate, ROA and manifest (ROAs and manifests carry two signatures); validators re-check all of it every sync. BGPsec signs every hop: 20 hops exceed even extended BGP messages.

2 SRv6

No room in the packet

SIDs ride in every packet; a 3,309 B signature can't, and per-packet signing was never used. PQ authentication must live in the control plane: policy channel and HMAC keys.

3 Agentic AI NetOps

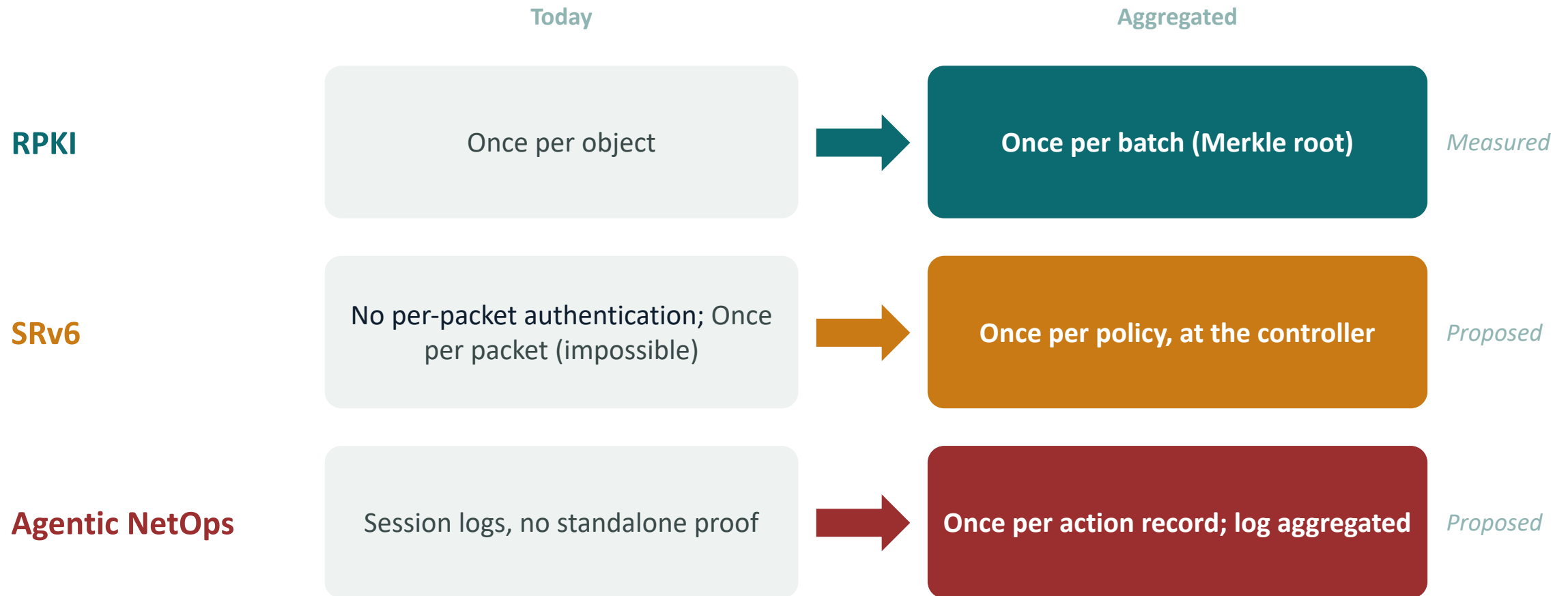
Proof must last for years

Agents can change the network without per-action human approval. Auditors need standalone proof of who did what, under which authority, verifiable offline years later.

Note: BGPsec is barely deployed (2 public keys in the RPKI, Oct 2025), so our measurement is on RPKI.

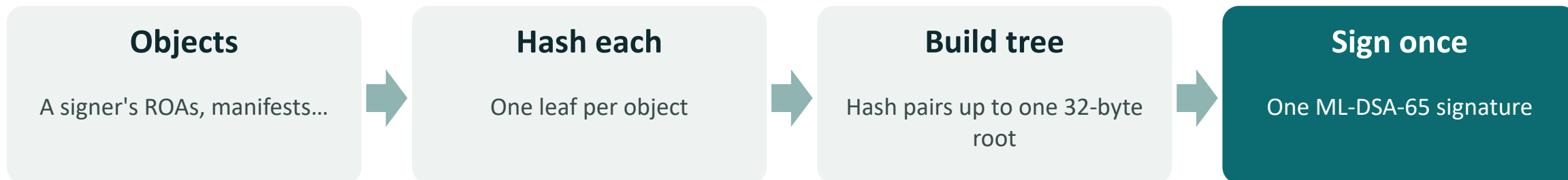
Carrier Networks: Aggregate the signature

Aggregate the Signature, don't multiply it. Move the signing boundary to where the cost amortises: one principle, three different mechanisms



RPKI: hash every object, sign one root

Builds on Merkle Tree Certificates, RPKI manifests and pqRPKI



A validator then either...

- Recomputes the root from the full set it already downloads: one signature check, no proofs
- Or checks one object with an inclusion proof: +33 B per tree level

Who signs in the real world?

- Each CA signs its own objects: ~10 on average, so most trees are small
- Big wins: large CAs, and a validator signing the VRP list it sends to routers (unsigned today)
- VRPs are computed by validators; nobody signs them

Result: signing stays flat

Scale test on live RPKI VRPs (liboqs / oqs-provider). Each row = a hypothetical signer with n objects.

Batch size n	Mean root sign (ms)	Per-object bundle (B)	Signatures
1	~10.7	3,309	1 → 1
100	~9.9	3,540	100 → 1
10,000	~9.0	3,771	10,000 → 1
100,000	~9.9	3,870	100,000 → 1
996,690	~10.0	3,969	996,690 → 1

~10 ms

signing, flat across six orders of magnitude

+33 B / level

3,969 B bundle at 20 levels (660 B proof)

1 vs n

signatures per batch

Key Points:

- Per object, the bundle is slightly bigger than one signature; the gain is at scale. Shipping every proof: ~5× fewer bytes (3.3 GB → 0.66 GB)
- Recomputing the root needs no proofs, but one missing object blocks the whole batch
- Not measured yet: verification time, signing variance, tree-build time (our question 1)

Proposals: SRv6 and agentic NetOps

Not yet measured; this is where we want the room's input

SRv6: sign the policy, not the packet

- Controller signs the policy once with ML-DSA-65
- Sent via BGP SR Policy or PCEP; head-end verifies once
- Packets carry a short symmetric token, like the SRH HMAC TLV
- HMAC is already quantum-resistant; open problems are key distribution and how long to trust cached state

Agents: a PQ-signed receipt per action

- Each action wrapped in COSE_Sign1 with ML-DSA (RFC 9964)
- Agent, scope, target and time all in the signed part
- Auditor verifies offline, years later, with no server
- Identity via MTAC draft; append-only logs via SCITT (RFC 9943)

Five questions for this workshop

Where operator, vendor and standards input is needed

1 RPKI at scale Impact on validation time and publication-to-router latency under realistic churn?

2 SRv6 cached state How long can a router trust cached policy if the controller is unreachable, given sub-50 ms fast reroute?

3 Action attestation Appetite for a lightweight COSE action-attestation profile, perhaps on SCITT?

4 Hardware Which HSM and route-processor gaps are firmware fixes, and which need new hardware?

5 Mixed validation How long must classical and PQ validation coexist, and at what cost to validator software?

Thank You!

IAB Workshop on Accelerating the Deployment of Post-Quantum Authentication (pqws), Prague, 11-12 October 2026

Jaypal Baviskar · Afshan Mulla
Technical Leader, Cisco CX (views our own)