Avahi

Encrypted today. Readable later.

Traffic on RSA or elliptic-curve key exchange can be recorded now and decrypted once a cryptographically relevant quantum computer exists. NIST names this harvest-now, decrypt-later threat as a main reason the transition is urgent.

THE DEADLINES ARE SET

August 2024
NIST publishes FIPS 203, 204, and 205

End of 2026
EU Member States begin the transition

December 31, 2030
Post-quantum key exchange on the most sensitive federal systems

December 31, 2031
Post-quantum signatures on those systems

After 2035
NIST disallows quantum-vulnerable algorithms

Sources: NIST FIPS 203, 204, and 205; NIST IR 8547 (October 27, 2026); Executive Order 14412 and OMB M-26-15; EU Coordinated Implementation Roadmap.

HOW THE ASSESSMENT WORKS

Every mandate starts with an inventory.

Fixed fee. Scope and timing set with each customer.

01

Discover and inventory

AWS KMS, AWS Certificate Manager, AWS Private CA, AWS CloudHSM, and TLS, VPN, and SSH settings. Then application code, open source dependencies, and container images.

DELIVERS
A cryptographic inventory your security team can maintain

02

Rank by quantum risk

- How long the data must stay confidential
- Exposure to record-now, decrypt-later collection
- Role as a long-lived root of trust

DELIVERS
A prioritized register of quantum-vulnerable cryptography

03

Sequence the roadmap

A plan for each prioritized finding, aligned to NIST FIPS 203, 204, and 205 and to the post-quantum capabilities AWS offers today.

DELIVERS
The remediation roadmap and a security leadership readout

ALREADY HANDLED BY AWS

Much of the work can start now.

- Hybrid post-quantum TLS on AWS KMS, AWS Certificate Manager, and AWS Secrets Manager endpoints
- Hybrid post-quantum TLS to Amazon CloudFront viewers

OWNED BY YOUR TEAM, SEQUENCED BY US

- Hybrid ML-KEM TLS on load balancers and APIs
- IAM guardrails that block downgrade
- ML-DSA for signing and private PKI
- Enforcement in infrastructure code
- SDK and TLS client upgrades
- Crypto-agile custom applications

WHEN TO START

A planned cloud migration, hardware refresh, or public key infrastructure (PKI) renewal is the natural point to build in post-quantum upgrades.

HOW WE WORK WITH YOU

Support is provided during the engagement. A named Avahi lead runs regular working sessions with your security team, with cadence agreed in scoping, and answers questions throughout.

© 2026 Avahi