

ML-DSA Certificate issuance and the managed-cloud gap

Chainguard builds container images, packages, and toolchains, and over the summer of 2026 we made that software ML-DSA capable end to end. We have ML-DSA certificate support in every Chainguard Containers `latest` tag, a compliance suite that performs real ML-DSA-87 TLS 1.3 handshakes, and a name-constrained ML-DSA-87 CA of our own with the services behind it upgraded. Then we tried to put an ML-DSA certificate on a managed cloud endpoint, and nothing would take it. The software half of post-quantum authentication is done. The infrastructure half, issuance and termination, is where deployment stops, and this paper documents exactly where.

As of September 2026 there is no public CA, staging or otherwise, that will issue an ML-DSA certificate, and no managed load balancer at AWS, Google Cloud, Azure, or Cloudflare that will terminate one. We are asking the CAs and cloud providers at this workshop for two things: a public test ACME server that issues ML-DSA certificates, and one managed load balancer that accepts them in beta. In return Chainguard will be the first deployer of both and publish what we measure.

Where it is blocked

Issuance. No public CA issues ML-DSA certificates, so Chainguard's own public endpoints still present RSA-2048. Let's Encrypt has committed to Merkle Tree Certificates, targeting a staging environment in late 2026 and production in 2027, and is tracking RFC 9881 rather than issuing against it. Google Cloud's roadmap lists ML-DSA in Certificate Authority Service as a future item with the signatures track targeted for the end of 2028. AWS Private CA has issued ML-DSA-44, -65, and -87 certificates since 10 November 2025 and is where our CA runs.

Termination. On Google Cloud, `gcloud compute ssl-certificates create` rejected the certificate with "The SSL certificate uses an unsupported algorithm. The loadbalancer supports RSA-2048 and ECDSA P-256 certificates," and `gcloud certificate-manager certificates create` rejected it with `INVALID_ARGUMENT: unsupported encryption algorithm` on the `self_managed` field (21 August 2026). On AWS, the load balancer in

us-east-2 did not accept the same certificate (24 August 2026). Both providers' load balancers already negotiate hybrid ML-KEM key exchange, so the gap is specific to authentication.

Trust stores and key formats. OpenSSL rejects RFC 9925 unsigned root certificates as an unknown signature algorithm; we opened [openssl/openssl#32391](#) on 14 August 2026 and it is in review. Go and the Go Cryptographic Module serialize ML-DSA and ML-KEM private keys in seed form, while the Chainguard FIPS provider for OpenSSL 3.6 imports only the semi-expanded form, so binaries that enabled the provider would have crashed until we added a fallback.

Challenges and Costs

The termination gap can be worked around by running our own TLS-terminating load balancer on Chainguard OS images. We build images; we do not want to operate load balancers. The issuance gap is worked around with a private CA that no party outside Chainguard trusts, which is why the public endpoints are still RSA.

What we are asking for

We recognise the IAB convenes rather than operates, so these asks are directed at the CAs and cloud providers in the room.

1. A public demo ACME server issuing ML-DSA X.509 certificates, outside any root program. Our proposed shape: seven-day certificates, mandatory DNS-01 validation and CAA, server-auth, client-auth, and code-signing profiles, with a CT log. Chainguard will ship an opt-in trust bundle for it in its images.
2. At least one managed load balancer and certificate manager that accepts self-managed ML-DSA certificates as an alpha or beta.
3. Follow-up on RFC 9925 unsigned-root verification and on an interoperable ML-DSA/ML-KEM private-key encoding across FIPS-validated and non-validated implementations.

We would like to hold up our end. For any test CA that emerges, Chainguard will ship an opt-in trust bundle in its images and publish Terraform and ACME examples against it, and we will run our compliance suite against the first managed load balancer that accepts ML-DSA and share the results.