

Use of ML-DSA in TLS 1.3

[draft-ietf-tls-mlds](#)

Tim Hollebeek, Sophie Schmieg, Bas Westerbaan

IETF 125 · TLS WG · Monday 16 March 2025

What This Draft Does (and Doesn't Do)

- Registers three ML-DSA SignatureScheme codepoints (ML-DSA-44, ML-DSA-65, ML-DSA-87)
- Specifies use in TLS 1.3 handshake signatures and certificate chains
- Prohibits use in TLS 1.2 and earlier
- **That's it. It's short.**
- Does NOT say you can't or shouldn't do hybrid — hybrid is simply out of scope

Request for WGLC

- Draft -01 published, no open issues, well-reviewed
- FIPS 204 is final — the algorithm is stable
- Draft is simple and uncontroversial — just codepoints and basic rules
- ML-DSA is already being deployed in the ecosystem
- Government/compliance deadlines are approaching
- **Let's not be the bottleneck**