Transport Layer Security則
Internet-Draft
Intended status: Informational
Expires: 23 September 2026

T. Hollebeek
DigiCert
S. Schmieg
Google
B. E. Westerbaan
Cloudflare

22 March 2026

Use of ML-DSA in TLS 1.3
draft-ietf-tls-mldsa-02

Abstract

This memo specifies how the post-quantum signature scheme ML-DSA (FIPS 204) is used for authentication in TLS 1.3.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://tlswg.github.io/tls-mldsa/draft-ietf-tls-mldsa.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-tls-mldsa/.

Discussion of this document takes place on the Transport Layer Security Working Group mailing list (mailto:tls@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/tls/. Subscribe at https://www.ietf.org/mailman/listinfo/tls/.

Source for this draft and an issue tracker can be found at https://github.com/tlswg/tls-mldsa.

Status of This Memo

This Internet-Draft will expire on 23 September 2026.

Table of Contents

1. Introduction 2
2. Conventions and Definitions 2
3. ML-DSA SignatureScheme values 3
3.1. Certificate chain 3
3.2. Handshake signature 3
3.3. TLS 1.2 4
4. Security Considerations 4
5. IANA Considerations 4
6. References 4
6.1. Normative References 4
6.2. Informative References 5
Acknowledgments 5
Authors' Addresses 5

1. Introduction

ML-DSA is a post-quantum module-lattice-based digital signature algorithm standardised by NIST in [FIPS204].

This memo specifies how ML-DSA can be negotiated for authentication in TLS 1.3 via the signature_algorithms and signature_algorithms_cert extensions.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. ML-DSA SignatureScheme values

As defined in [RFC8446], the SignatureScheme namespace is used for the negotiation of signature scheme for authentication via the signature_algorithms and signature_algorithms_cert extensions. This document adds three new SignatureScheme values for the three ML-DSA parameter sets from [FIPS204] as follows.

SignatureScheme	FIPS 204	Certificate AlgorithmIdentifier
mldsa44(0x0904)	ML-DSA-44	id-ML-DSA-44 (2.16.840.1.101.3.4.3.17)
mldsa65(0x0905)	ML-DSA-65	id-ML-DSA-64 (2.16.840.1.101.3.4.3.18)
mldsa87(0x0906)	ML-DSA-87	id-ML-DSA-87 (2.16.840.1.101.3.4.3.19)

Table 1: SignatureSchemes for ML-DSA

Note that these are different from the HashML-DSA pre-hashed variants defined in Section 5.4 of [FIPS204].

3.1. Certificate chain

For the purpose of signalling support for signatures on certificates as per Section 4.2.3 of [RFC8446], these values indicate support for signing using the given AlgorithmIdentifier shown in Table 1 as defined in [MLDSACERTS].

3.2. Handshake signature

When one of those SignatureScheme values is used in a CertificateVerify message, then the signature MUST be computed and verified as specified in Section 4.4.3 of [RFC8446], and the corresponding end-entity certificate MUST use the corresponding AlgorithmIdentifier from Table 1.

If the signature or public key is of the wrong length, the client MUST treat this a verification failure, and thus terminate the handshake with decrypt_error alert.

The context parameter defined in [FIPS204] Algorithm 2 and 3 MUST be the empty string. Note that the context parameter of FIPS 204 is different from the context string of Section 4.4.3 of [RFC8446].

3.3. TLS 1.2

The schemes defined in this document MUST NOT be used in TLS 1.2 [RFC5246] or earlier versions. A peer that receives ServerKeyExchange or CertificateVerify message in a TLS 1.2 connection with schemes defined in this document MUST abort the connection with an illegal_parameter alert.

4. Security Considerations

The security considerations of [RFC8446] (eg. appendices C.2, E.1 and Section 4.4.3) and [FIPS204] (Section 3.4 and 3.6) apply.

5. IANA Considerations

This document requests new entries to the TLS SignatureScheme registry, according to the procedures in Section 6 of [TLSIANA].

Value	Description	Recommended	Reference
0x0904	mldsa44	N	This document.
0x0905	mldsa65	N	This document.
0x0906	mldsa87	N	This document.

Table 2

6. References

6.1. Normative References

[FIPS204] "Module-lattice-based digital signature standard", National Institute of Standards and Technology (U.S.), DOI 10.6028/nist.fips.204, August 2024, <https://doi.org/10.6028/nist.fips.204>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

6.2. Informative References

[MLDSACERTS] Massimo, J., Kampanakis, P., Turner, S., and B. Westerbaan, "Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA)", Work in Progress, Internet-Draft, draft-ietf-lamps-dilithium-certificates-13, 30 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-dilithium-certificates-13>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/rfc/rfc5246>.

[TLSIANA] Salowey, J. A. and S. Turner, "IANA Registry Updates for TLS and DTLS", Work in Progress, Internet-Draft, draft-ietf-tls-rfc8447bis-15, 21 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-rfc8447bis-15>.

Acknowledgments

Thanks to Alicja Kario, John Mattsson, Rebecca Guthrie, Alexander Bokovoy, Niklas Block, Ryan Appel, Loganaden Velvindron, and Nick Sullivan for their review and feedback.

Authors' Addresses

Tim Hollebeek
DigiCert
Email: tim.hollebeek@digicert.com

Sophie Schmieg
Google
Email: sschmieg@google.com

Bas Westerbaan
Cloudflare
Email: bas@cloudflare.com