TLS
Internet-Draft
Intended status: Informational
Expires: 13 November 2026

M. Chen
China Mobile
X. Song
ZTE Corp.

12 May 2026

Use of Composite FN-DSA Signatures in TLS 1.3
draft-chen-tls-composite-fndsa-00

Abstract

Compositing the post-quantum FN-DSA signature with traditional signature algorithms provides protection against potential breaks in either component. This document specifies how such a composite signature can be used for authentication in TLS 1.3. The selection of composite algorithms is intentionally chosen to strictly mirror the composite strategies for ML-DSA. This alignment provides two distinct and predictable security tiers for hybrid signatures, ensuring a consistent approach to post-quantum transition across the ecosystem.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 13 November 2026.

Copyright Notice

Table of Contents

1. Introduction

The advent of quantum computing poses a significant threat to current cryptographic systems. During the transition to post-quantum cryptography (PQC), cautious implementers may opt to combine cryptographic algorithms such that an attacker would need to break all of them simultaneously to compromise the protected data. These mechanisms are referred to as Post-Quantum/Traditional (PQ/T) Hybrids [RFC9794].

One practical way to implement a hybrid signature scheme is through a composite signature algorithm. In this approach, the composite signature consists of two signature components, each produced by a different signature algorithm.

FN-DSA [FIPS206] is a post-quantum signature scheme standardized by NIST. This memo specifies how a composite FN-DSA signature can be negotiated for authentication in TLS 1.3 via the "signature_algorithms" and "signature_algorithms_cert" extensions.

The composite algorithms defined herein are based on the framework specified in [I-D.chen-lamps-fndsa-composite-sigs]. A key design goal of this specification is to ensure *consistency across the emerging post-quantum ecosystem*. To that end, the selection of algorithm pairings in this document is intentionally aligned with the choices made for ML-DSA in draft-ietf-lamps-pq-composite-sigs. This creates two clear security tiers, allowing organizations to treat FN-DSA and ML-DSA composites at the same security level as interchangeable from a policy perspective.

1.1. Conventions and Terminology

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].

"Composite FN-DSA" refers to a composite FN-DSA signature scheme as defined in [I-D.chen-lamps-fndsa-composite-sigs]. For brevity, this document uses fndsa512 and fndsa1024 in SignatureScheme names to refer to the Falcon-padded-512 and Falcon-padded-1024 variants, respectively.

2. Composite FN-DSA SignatureSchemes

As defined in [RFC8446], the SignatureScheme namespace is used for the negotiation of signature schemes. This document adds new SignatureScheme values for composite FN-DSA, organized into two tiers that mirror the ML-DSA composite strategy.

```
enum {
    /* Tier 1 Composites (FN-DSA-512 based, mimicking ML-DSA-44) */
    fndsa512_rsa2048_pss_sha256(TBD1),
    fndsa512_ecdsa_p256_sha256(TBD2),
    fndsa512_ed25519(TBD3),

    /* Tier 2 Composites (FN-DSA-1024 based, mimicking ML-DSA-87) */
    fndsa1024_rsa3072_pss_sha512(TBD4),
    fndsa1024_ecdsa_p384_sha512(TBD5),
    fndsa1024_ecdsa_p521_sha512(TBD6),
    fndsa1024_ecdsa_brainpoolP384r1_sha512(TBD7),
    fndsa1024_ed448(TBD8),

} SignatureScheme;
```

Composite FN-DSA is treated as an opaque signature algorithm, similar to the "PureEdDSA" algorithms in TLS 1.3 (Section 4.2.3 of [RFC8446]). Any hash functions used are internal to the composite algorithm itself, as specified in [I-D.chen-lamps-fndsa-composite-sigs].

When a composite FN-DSA signature scheme is used in TLS, the signing and verification operations MUST be performed on the input data as constructed by TLS (Section 4.4.3 of [RFC8446]). This input is then passed to the composite signature primitive, which applies its own internal domain separation.

When a composite FN-DSA SignatureScheme is negotiated, the end-entity certificate presented in the TLS handshake MUST contain a public key compatible with that SignatureScheme.

The schemes defined in this document MUST NOT be used in TLS 1.2 [RFC5246].

3. Signature Algorithm Restrictions

The composite algorithms defined in this document are suitable for use in both the signature_algorithms and signature_algorithms_cert extensions. Consistent with TLS 1.3’s requirements, all defined RSA-based composites use the RSASSA-PSS padding scheme for handshake signatures. Certificates MAY be signed with composites using RSASSA-PKCS1-v1_5, but these are not negotiated for use in the TLS CertificateVerify message.

4. Selection Criteria for Composite Signature Algorithms

The composite signatures specified in this document are a curated set of cryptographic pairs, directly adopted from [I-D.chen-lamps-fndsa-composite-sigs]. The selection process was guided by a single, overriding principle:

* *Strictly Mirroring ML-DSA Composite Strategy:* The pairings for fndsa512 are identical to those for ML-DSA-44, and the pairings for fndsa1024 are identical to those for ML-DSA-87, as defined in draft-ietf-lamps-pq-composite-sigs.

This prescriptive approach ensures a consistent, two-tiered security model across the PQC signature landscape, simplifying policy development and promoting interoperability.

4.1. Mapping TLS SignatureSchemes to Composite FN-DSA

The following table provides a mapping between the TLS SignatureScheme identifiers and the corresponding composite algorithm identifiers from [I-D.chen-lamps-fndsa-composite-sigs].

TLS SignatureScheme	Composite FN-DSA OID Name
fndsa512_rsa2048_pss_sha256	id-fnpadded512-rsa2048-pss-sha256
fndsa512_ecdsa_p256_sha256	id-fnpadded512-ecdsa-p256-sha256
fndsa512_ed25519	id-fnpadded512-ed25519-sha512
fndsa1024_rsa3072_pss_sha512	id-fnpadded1024-rsa3072-pss-sha512
fndsa1024_ecdsa_p384_sha512	id-fnpadded1024-ecdsa-p384-sha512
fndsa1024_ecdsa_p521_sha512	id-fnpadded1024-ecdsa-p521-sha512
fndsa1024_ecdsa_brainpoolP384r1_sha512	id-fnpadded1024-ecdsa-brainpoolP384r1-sha512
fndsa1024_ed448	id-fnpadded1024-ed448-shake256

Table 1: Mapping TLS SignatureSchemes to Composite FN-DSA Identifiers

5. Security Considerations

The security considerations discussed in [I-D.chen-lamps-fndsa-composite-sigs] apply. The primary goal is to provide hybrid security, where the composite signature remains secure as long as at least one component algorithm remains secure.

Composite signature schemes do not in general preserve strong unforgeability (SUF-CMA) once the traditional component is broken. This does not impact TLS, which relies on existential unforgeability (EUF-CMA).

TLS clients that support both post-quantum and traditional-only signature algorithms are vulnerable to downgrade attacks. The continuity mechanism defined in [I-D.sheffer-tls-pqc-continuity] can be used to mitigate this risk.

6. IANA Considerations

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

Value	Description	Recommended	Reference
TBD1	fndsa512_rsa2048_pss_sha256	N	This document.
TBD2	fndsa512_ecdsa_p256_sha256	Y	This document.
TBD3	fndsa512_ed25519	N	This document.
TBD4	fndsa1024_rsa3072_pss_sha512	N	This document.
TBD5	fndsa1024_ecdsa_p384_sha512	N	This document.
TBD6	fndsa1024_ecdsa_p521_sha512	N	This document.
TBD7	fndsa1024_ecdsa_brainpoolP384r1_sha512	N	This document.
TBD8	fndsa1024_ed448	N	This document.

Table 2: Additions to TLS SignatureScheme Registry

7. References

7.1. Normative References

[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>.

[I-D.chen-lamps-fndsa-composite-sigs] Chen, M., "Composite FN-DSA for use in X.509 Public Key Infrastructure", 8 May 2026.

[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>.

7.2. Informative References

[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>.

[RFC9794] Driscoll, F., Parsons, M., and B. Hale, "Terminology for Post-Quantum Traditional Hybrid Schemes", RFC 9794, DOI 10.17487/RFC9794, June 2025, <https://www.rfc-editor.org/rfc/rfc9794>.

[FIPS206] National Institute of Standards and Technology (NIST), "FIPS 206, Fast-Fourier-Transform-based Digital Signature Algorithm", n.d., <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>.

[I-D.sheffer-tls-pqc-continuity] Sheffer, Y. and T. Reddy.K, "PQC Continuity - Downgrade Protection for TLS Servers Migrating to PQC", Work in Progress, Internet-Draft, draft-sheffer-tls-pqc-continuity-00, 18 October 2025, <https://datatracker.ietf.org/doc/html/draft-sheffer-tls-pqc-continuity-00>.

Appendix A. Acknowledgments

This document also draws on draft-reddy-tls-composite-mldsa. Thanks to the authors of that document.

Authors' Addresses

Meiling Chen
China Mobile
BeiJing
China
Email: chenmeiling@chinamobile.com

Xueyan Song
ZTE Corp.
Email: song.xueyan2@zte.com.cn