TLS
Internet-Draft
Intended status: Informational
Expires: 7 November 2026

X. Song
ZTE Corp.
M. Chen
China Mobile

6 May 2026

Use of FN-DSA in TLS 1.3
draft-song-ietf-tls-fndsa-00

Abstract

NIST is standardizing FN-DSA as a post-quantum NTRU-lattice-based digital signature algorithm, which is expected to be published in FIPS 206. This document specifies how FN-DSA can be negotiated for authentication in TLS 1.3 via the signature_algorithms and signature_algorithms_cert extensions.

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 7 November 2026.

Table of Contents

1. Introduction

FN-DSA (formerly known as Falcon) is a lattice-based digital signature scheme based on the Gentry-Peikert-Vaikuntanathan (GPV) hash-and-sign framework, instantiated over NTRU lattices with fast Fourier sampling techniques. The core hard problem underlying FN-DSA is the Short Integer Solution (SIS) problem over NTRU lattices. FN-DSA offers compact signatures and public keys compared to other post-quantum signature schemes. For bandwidth-constrained applications where signature size is a critical factor, FN-DSA provides a favourable alternative to ML-DSA and SLH-DSA.

Editor's Note: The FN-DSA description of the whole text needs double check after FIPS206 publishment.

This document specifies how FN-DSA is used for authentication in TLS 1.3, including certificate chain signatures and handshake signatures in the CertificateVerify message.

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. FN-DSA Signature Scheme 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 two new SignatureScheme values for the two FN-DSA parameter sets from [FIPS206] as follows.

SignatureScheme	FIPS 206	Certificate AlgorithmIdentifier
fndsa512(TBD1)	FN-DSA-512	id-FN-DSA-512 (2.16.840.1.101.3.4.3.TBD2)
fndsa1024(TBD3)	FN-DSA-1024	id-FN-DSA-1024 (2.16.840.1.101.3.4.3.TBD4)

Table 1: SignatureSchemes for FN-DSA

Note that these are the pure (non-pre-hashed) variants of FN-DSA. Pre-hashed variants are not defined in this document. This design choice follows the convention established by IETF for other post-quantum signature algorithms in protocol bindings. As discussed in [I-D.turner-lamps-cms-fn-dsa], when signature algorithms such as EdDSA, SLH-DSA, ML-DSA, and FN-DSA are used in protocol contexts where the data to be signed is typically small (such as TLS handshake transcripts or CMS signed attributes), the pre-hash mode offers no significant benefit in reducing the size of data to be signed.

3.1. Key and Signature Sizes

The following table summarizes the sizes of FN-DSA public keys and signatures for each parameter set, as defined in [FIPS206]. Two security levels of FN-DSA are recommended in this document. FN-DSA-512 is expected to offer a security level equivalent to NIST level 1. FN-DSA-1024 is expected to offer a security level equivalent to NIST level 5.

Parameter Set	Public Key (bytes)	Signature (bytes)
FN-DSA-512	897	666
FN-DSA-1024	1793	1280

Table 2: Key and Signature Sizes for FN-DSA

3.2. 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 [I-D.turner-lamps-fn-dsa-certificates].

Implementations SHOULD validate that the public key in the end-entity certificate matches the expected size for the negotiated parameter set. A mismatch MUST be treated as a verification failure.

3.3. 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 as a verification failure, and thus terminate the handshake with a decrypt_error alert.

The random salt used in FN-DSA signature generation MUST be derived from a cryptographically secure random number generator. Lack of fresh random data during FN-DSA signature generation leads to a differential fault attack [BD23].

4. Security Considerations

The security considerations of [RFC8446] and [FIPS206] apply.

Editor’s Note: This section should be expanded with FN-DSA-specific security considerations, including: random number generation requirements (see [BD23]), floating-point arithmetic implementation concerns, and side-channel attack mitigations. Specific references to [FIPS206] should be added once it is finalized.

5. IANA Considerations

This document requests new entries to the TLS SignatureScheme registry, according to the procedures in [RFC9847].

Value	Description	Reconmmended	Reference
TBD1	fndsa512	N	This document
TBD3	fndsa1024	N	This document

Table 3: TLS SignatureScheme Values for FN-DSA

6. Acknowledgements

TBD.

7. References

7.1. Normative References

[FIPS206] "Fast Fourier Transform over NTRU-Lattice-Based Digital Signature Algorithm", n.d., <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>.

[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>.

7.2. Informative References

[BD23] Bauer, S. and F. D. Santis, "A Differential Fault Attack against Deterministic Falcon Signatures", 2023, <https://eprint.iacr.org/2023/422>.

[I-D.turner-lamps-cms-fn-dsa]
Van Geest, D., Kampanakis, P., Turner, S., and B. Westerbaan, "Use of the FN-DSA Signature Algorithm in the Cryptographic Message Syntax (CMS)", Work in Progress, Internet-Draft, draft-turner-lamps-cms-fn-dsa-00, September 2025, <https://datatracker.ietf.org/doc/html/draft-turner-lamps-cms-fn-dsa-00>.

[I-D.turner-lamps-fn-dsa-certificates]
Massimo, J., "Internet X.509 Public Key Infrastructure -- Algorithm Identifiers for the Fast-Fourier Transform over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA)", Work in Progress, Internet-Draft, draft-turner-lamps-fn-dsa-certificates-00, November 2025, <https://datatracker.ietf.org/doc/html/draft-turner-lamps-fn-dsa-certificates-00>.

[RFC9847] Salowey, J. and S. Turner, "IANA Registry Updates for TLS and DTLS", RFC 9847, DOI 10.17487/RFC9847, December 2025, <https://www.rfc-editor.org/rfc/rfc9847>.

Authors' Addresses

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

Meiling Chen
China Mobile
Email: chenmeiling@chinamobile.com