Network Working Group
Internet-Draft
Intended status: Experimental
Expires: 3 September 2026

A. Maurette
IUT R&T B辿thune

2 March 2026

HMTFTP: HKDF-Derived TFTP with Optional AEAD Protection
draft-maurette-hmtftp-05

Abstract

HMTFTP is a lightweight UDP file transfer protocol derived from TFTP that adds TLV-based negotiation and an optional AEAD protection mode for DATA payloads. This document requests IANA actions: assignment of a service name and UDP port, and creation of registries for TLV Types, OpCodes, and Ciphersuites.

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 3 September 2026.

Table of Contents

1. Introduction

HMTFTP extends TFTP ([RFC1350]) with TLV-based negotiation and optional AEAD protection.

Cryptographic keys are derived using HKDF ([RFC5869]).

2. Relationship to TFTP

HMTFTP reuses TFTP message types and semantics ([RFC1350]) and OACK ([RFC2347]).

* Dedicated UDP port assigned by IANA

* TLV negotiation in RRQ/WRQ/OACK

* Optional AEAD protection

3. Transport

HMTFTP runs over UDP. The port number is assigned by IANA. Implementations MUST allow configuration.

Servers MAY respond from a different UDP port for the transfer.

4. TLV Processing Rules

TLVs MAY appear only in RRQ, WRQ, and OACK. TLVs MUST NOT appear in DATA, ACK, or ERROR.

TLVs MUST be processed in the order received. Duplicate TLVs MUST cause rejection unless explicitly allowed.

Unknown TLVs with Critical=1 MUST cause rejection. Unknown TLVs with Critical=0 MUST be ignored.

TLVs MUST NOT influence cryptographic processing unless explicitly defined as such.

5. Optional AEAD Security Mode

5.1. Key Derivation

The AEAD algorithm used by this specification is AES-256-GCM, as defined in [RFC5116].

IKM = PSK. salt = CNONCE || SNONCE. info = "hmtftp keys v1". OKM length = 44 octets.

5.2. Nonce Construction

nonce = iv_base[0..7] || uint32(n).

The 64-bit prefix is derived via HKDF and unique per session. The 32-bit counter guarantees uniqueness within session, provided wrap is prevented.

This construction ensures nonce uniqueness across sessions and within a session.

Retransmissions MUST reuse identical nonce and ciphertext.

5.3. BLKSIZE Constraints

In AEAD mode, total UDP payload = 4-byte header + BLKSIZE + 16-byte tag.

Implementations MUST ensure the datagram does not exceed path MTU. When unknown, total payload SHOULD NOT exceed 1200 bytes.

5.4. Limits

Block number wrap MUST NOT occur. Transfers MUST terminate before 65535 blocks.

6. IANA Considerations

6.1. Service Name and UDP Port

IANA is requested to assign:

This request follows the procedures in [RFC6335].

* Service Name: hmtftp
* Transport: udp
* Port: TBD

6.2. Registries

IANA is requested to create registries for TLV Types, OpCodes, and Ciphersuites (Expert Review, [RFC8126]).

7. Security Considerations

Without security mode, HMTFTP is vulnerable to spoofing and modification.

Implementations SHOULD follow UDP usage guidance ([RFC8085]).

Downgrade attacks are possible if ENC_REQ is not marked Critical. Clients requiring AEAD MUST set Critical=1.

Reflection and amplification attacks are possible. Implementations SHOULD limit response size prior to completing negotiation and SHOULD apply rate limiting.

Nonce reuse in AES-GCM is catastrophic. Implementations MUST enforce uniqueness and block limits.

8. Implementation Status

No interoperable public implementations are known.

Provided in accordance with [RFC7942].

9. Normative References

[RFC1350] Sollins, K., "The TFTP Protocol (Revision 2)", STD 33, RFC 1350, DOI 10.17487/RFC1350, July 1992, <https://www.rfc-editor.org/info/rfc1350>.

[RFC2347] Malkin, G. and A. Harkin, "TFTP Option Extension", RFC 2347, DOI 10.17487/RFC2347, May 1998, <https://www.rfc-editor.org/info/rfc2347>.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, DOI 10.17487/RFC5116, January 2008, <https://www.rfc-editor.org/info/rfc5116>.

[RFC5869] Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", RFC 5869, DOI 10.17487/RFC5869, May 2010, <https://www.rfc-editor.org/info/rfc5869>.

[RFC6335] Cotton, M., Eggert, L., Touch, J., Westerlund, M., and S. Cheshire, "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry", BCP 165, RFC 6335, DOI 10.17487/RFC6335, August 2011, <https://www.rfc-editor.org/info/rfc6335>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8085] Eggert, L., Fairhurst, G., and G. Shepherd, "UDP Usage Guidelines", BCP 145, RFC 8085, DOI 10.17487/RFC8085, March 2017, <https://www.rfc-editor.org/info/rfc8085>.

10. Informative References

[RFC7942] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", BCP 205, RFC 7942, DOI 10.17487/RFC7942, July 2016, <https://www.rfc-editor.org/info/rfc7942>.

Author’s Address

A. Maurette
IUT R&T B辿thune
France
Email: contact@c4tz.fr