

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: 1 September 2025

J. Hoyland  
Cloudflare  
February 2025

TLS Flag - Request mTLS  
draft-jhoyla-req-mtls-flag-02

## Abstract

Normally in TLS there is no way for the client to signal to the server that it has been configured with a certificate suitable for mTLS. This document defines a TLS Flag [I-D.ietf-tls-tlsflags] that enables clients to provide this hint.

## 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://jhoyla.github.io/draft-jhoyla-req-mtls-flag/draft-jhoyla-req-mtls-flag.html>. Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-jhoyla-req-mtls-flag/>.

Source for this draft and an issue tracker can be found at <https://github.com/jhoyla/draft-jhoyla-req-mtls-flag>.

## 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 5 August 2025.

## Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Conventions and Definitions . . . . .	2
3. Flag specification . . . . .	3
4. Security Considerations . . . . .	3
5. IANA Considerations . . . . .	3
6. Normative References . . . . .	3
Acknowledgments . . . . .	4
Author's Address . . . . .	4

## 1. Introduction

This document specifies a TLS Flag that indicates to the server that the client supports mTLS. Sometimes a server does not want to negotiate mTLS with every client, but might wish to authenticate a subset of them. In TLS 1.3 this may be done with post-handshake auth, however this adds an extra round-trip, and requires negotiation at the application layer. A client sending the request mTLS flag in the ClientHello allows the server to request authentication during the initial handshake only when it receives a hint the client supports it. This enables a number of use cases, for example allowing bots to authenticate themselves when mixed in with general traffic.

## 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. Flag specification

A server receiving this flag MAY send a CertificateRequest message.

### 4. Security Considerations

This flag should have no effect on the security of TLS, as the server may always send a CertificateRequest message during the handshake. This flag merely provides a hint that the client will be able to fulfil the request. If the client sets this flag but then fails to provide a certificate the server MAY terminate the connection with a bad\_certificate error.

### 5. IANA Considerations

This document requests IANA to add an entry to the TLS Flags registry in the TLS namespace with the following values:

- \* Value shall be TBD
- \* Flag Name shall be request\_mtls.
- \* Message shall be CH
- \* Recommended shall be set to no (N)
- \* The reference shall be this document {!draft-jhoyla-req-mtls}

### 6. Normative References

#### [I-D.ietf-tls-tlsflags]

Nir, Y., "A Flags Extension for TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-tlsflags-14, 13 September 2024, <<https://datatracker.ietf.org/doc/html/draft-ietf-tls-tlsflags-14>>.

[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>>.

#### Acknowledgments

TODO acknowledge.

#### Author's Address

Jonathan Hoyland  
Cloudflare  
Email: jonathan.hoyland@gmail.com