TLS Ticket Request Message
draft-rashok-tls-ticket-request-msg-00

Abstract

TLS session ticket provides a stateless mechanism for server to resume connection with client. As per TLS 1.3 [RFC8446], server always sends arbitrary number of session ticket after handshake. This document introduces a new message which is TicketRequest message, it can be send by client after handshake at any point of connection lifetime to retrieve session ticket. The proposed mechanism in this document is only for TLS 1.3 and DTLS 1.3 and future versions.

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 June 22, 2020.

Copyright Notice

Copyright (c) 2019 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 Simplified BSD License text as described in Section 4.e of
1. Introduction

As per TLS 1.3 [RFC8446], TLS server sends arbitrary number of session ticket after handshake (or after post-handshake authentication). Such session tickets are needed only for a client which resumes parallel connections to server immediately. But this delays the application data processing for a client which is not going to resume parallel connections immediately. Such clients might need session ticket at later point of time or it may not need also.

So a client’s need based session ticket generation will be more efficient on both server and client.

To achieve this a new TicketRequest message is proposed in this specification, which should be send by client as and when it needs session ticket for resumption.

1.1. Requirements Language

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 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. SessionTicket Generation

Client should be able to retrieve session ticket from server in two ways

1. Immediately after handshake or after post-handshake authentication.
By sending TicketRequest message to server at later time during data transfer.

A new ticket_request extension [I-D.ietf-tls-ticketrequests] has been proposed to give control over client to request the amount of session ticket it needs for resuming parallel connection immediately after handshake.

This extension SHOULD be send by client with TicketRequestContents.count as zero, if it does not need to resume parallel connection immediately after handshake. Then it can use TicketRequest message at later point when it needs to resume connection.

A client can send any number of TicketRequest message in its connection lifetime with server. But server SHOULD limit the total number of ticket issued to client per connection to prevent DOS attack.

3. TicketRequest Message

TicketRequest message send by client holds the count parameter, which indicates how much session ticket immediately client needs.

Structure of this message:

```c
struct {
    uint8 count;
} TicketRequest;
```

count  The number of tickets needed by client

4. IANA Considerations

Needs to register new TLS message type TicketRequest in IANA

5. Security Considerations

The amount of ticket requested per connection should be limited by threshold value at server to prevent DOS attack.

6. References

6.1. Normative References
[I-D.ietf-tls-ticketrequests]


6.2. Informative References

[I-D.ietf-tls-dtls13]


Author’s Address

Raja Ashok
Huawei
Whitefield
Bengaluru, Karnataka 560037
India

Email: rashok.ietf@gmail.com