TLS Ticket Requests

draft-wood-tls-ticket-requests

Tommy Pauly (tfpauly@apple.com)
David Schinazi (dschinazi@apple.com)
Christopher A. Wood (cawood@apple.com)

TLS
IETF 102, July 2018, Montreal

Problem

Servers vend a fixed number of tickets to clients upon connection establishment

Some clients may want or need more tickets

- Parallel connections, Happy Eyeballs V2-style racing, connection priming

Some tickets simply go to waste

Approach

Allow clients to request tickets on demand, post handshake

- Requests carry an identifier and optional context to match with NewSessionTicket extensions

  Clients opt-in via new ticket_request extension

  Servers do not send NewSessionTickets (NSTs) unless requested

Alternative Design

Clients send an extension that signals the number of tickets desired in the CH

- Does not allow for dynamic vending of tickets
- Avoids adding post handshake messages

Utility

Ticket request utility depends entirely upon how many tickets clients need

- If few tickets are ever requested, servers should probably increase the number of NSTs minted

Note: ticket vending can be accomplished today if servers vend more than one NST per connection

- Avoid hacks and waste by making ticket requests explicit

Questions?

WG Interest?