TLS Flags Extension

Yoav nir

IETF 108

TL;DR Version

- The flags extension carries a bitstring of flags. The flags themselves will be in an IANA registry.
- Each flag indicates that some feature is enabled or some attribute is supported.
- Extension is as short as the highest-number set flag will allow.
  - IANA registry policy attempts to make the commonly-used flags have a low number.
- Flags appear in ClientHello. Server responds in ServerHello or EncrpytedExtensions
  - The document for the particular extension decides.

Since we last talked about this…

- Eliminated the option for server to resond unsolicited.
- Clarified that we support up to 2040 flags. Should be plenty.
- IANA Expert guidance
- Clarification of error handling

- Bottom line: Think it’s ready.

Question for the ”room”

- Suggestion from Hannes Tschofenig: “Wouldn’t you want to register a flag for "Post-Handshake Client Authentication" in this document?”
- This is a current flag that is defined in the TLS 1.3 base document (RFC 8446)
- The good: we don’t start out with an empty registry.
- The bad: we will have two ways of saying the same thing.
  - Since the client can’t know that the server supports tls-flags, can it afford to not send the extension defined in 8446?
- So far, I haven’t added it.