Resumption across SNI

draft-vvv-tls-cross-sni-resumption

IETF 108 (virtual)

Is session resumption allowed when SNI changes?

RFC 8446, Section 4.6.1:

“Clients MUST only resume if the new SNI value is valid for the server certificate presented in the original session and SHOULD only resume if the SNI value matches the one used in the original session. The latter is a performance optimization: normally, there is no reason to expect that different servers covered by a single certificate would be able to accept each other's tickets; hence, attempting resumption in that case would waste a single-use ticket. If such an indication is provided (externally or by any other means), clients MAY resume with a different SNI value.”

Is session resumption allowed when SNI changes?

RFC 8446, Section 4.6.1:

“Clients MUST only resume if the new SNI value is valid for the server certificate presented in the original session and SHOULD only resume if the SNI value matches the one used in the original session. The latter is a performance optimization: normally, there is no reason to expect that different servers covered by a single certificate would be able to accept each other's tickets; hence, attempting resumption in that case would waste a single-use ticket. If such an indication is provided (externally or by any other means), clients MAY resume with a different SNI value.”

An indication

The proposed draft defines an empty NewSessionTicket extension.

“If the extension is sent, it indicates that the client MAY use the ticket for any SNI value for which the certificate presented by the server is valid. [...]

The server MAY send the extension if it reasonably believes that any server for any identity presented in its certificate would be capable of accepting that ticket. The server SHOULD NOT send the extension otherwise, since, if the client follows the single-use ticket policy recommended by [RFC8446], sending the ticket results in it being no longer usable regardless of whether resumption has succeeded.”

Discussion