SHA-1

In TLS: no, in chain: for a little while

How do we ensure that “a little while” isn’t “forever”?

Use signature_algorithms

… if sha1 isn’t in signature_algorithms, it’s not cool

Alternative view: signature_algorithms should not dictate certificate chain choice

… trust in the chain is someone else’s problem

… servers will just send what they have