TLS 1.2 is frozen

Rich Salz, Nimrod Aviram
As promised ...

• I committed at IETF 116 to write a draft freezing TLS 1.2

• “No new changes,” but maybe deprecations as attacks get stronger

• Thanks to Nimrod for joining as co-author and making many improvements
Content

• No new algorithms

• Can register ALPN and key exporter labels

• Otherwise, no new registry entries of any kind

• Annotation that new ones are “For TLS 1.3 or later”
  • We need a new column in the registries

... this implies no post-quantum
Impact on other protocols

• New protocols MUST say TLS 1.3

• If deployment considerations are a concern, MAY also say TLS 1.2
Next steps

• Request adoption by the WG

• This is probably ready for WGLC