Transport Layer Security (TLS) Cached Information Extension

S. Santesson, H. Tschofenig
Problem Statement

• TLS handshakes often include fairly static information, such as the server certificate and a list of trusted Certification Authorities (CAs).

• This document defines an extension that omits the exchange of already available information.

• The TLS client informs a server of cached information.
Document Content

• CachedObject object is sent in ClientHello
• ServerHello returns CachedObject
• Instead of sending the Certificate payload with the certs in it only the fingerprint is sent.
  – Same for list of Trusted Cas
• Cached Object contains:
  – Type: certificate_chain(1), trusted_cas(2)
  – Hash Algorithm
  – Hash Value
Next Steps?

• More reviews needed.