TLS Out-of-Band Public Key Validation

P. Wouters, J. Gilmore, S. Weiler, T. Kivinen, H. Tschofenig
Status

• After the Taipei IETF meeting we had published 3 draft version.

• Review comments lead to a number of changes:
  – Moved the support for hashes of public keys to [I-D.ietf-tls-cached-info]
  – Changed description throughout the entire document.

• We would like to thank Martin Rex, Bill Frantz, Zach Shelby, Carsten Bormann, Cullen Jennings, Rene Struik, Alper Yegin, and Jim Schaad.
How does it work?

client_hello, cert_type="RawPublicKey" ->

<- server_hello, cert_type="RawPublicKey", certificate, server_key_exchange, certificate_request, server_hello_done

certificate, client_key_exchange, certificate_verify, change_cipher_spec, finished ->

<- change_cipher_spec, finished

Cert_type is defined in RFC 6091

Certificate payload only contains SubjectPublicKeyInfo structure

Application Data <-> Application Data
Next steps?

• We believe it is ready for a WGLC.