Out-of-Band Public Key Validation for Transport Layer Security (TLS)

draft-ietf-tls-oob-pubkey-06.txt

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

Main Changes

- Most recent update incorporated feedback from last meeting.
- Roll-back to version -03
  - (and thereby skipping major changes introduced in version -04)
- Clarifications regarding the usage of SubjectPublicKeyInfo.
  - Klaus Hartke was working on an implementation and had questions regarding the encoding of SubjectPublicKeyInfo in the certificate payload.
- Removed dependency to RFC 6091
  - Defined a new parameter certificate_type (instead of cert_type).
  - No support for OpenPGP specified.
  - Added a new certificate type registry.

What's Next?

- Is the new certificate_type approach acceptable?
- Is it OK to remove OpenPGP support from the document?