IETF 86

EST update

v.2

What happened with 85-86 mid-updates?

- We claimed an update for a specific date
  - People laughed
  - My apologies for missing the date
- Now I know why
  - Putting out a date got us lots of comments
  - Thanks!

-04 was published

-05 was published

-06 polishing actions (ongoing)

-05 Highlights

- Substantial tightening of prose
- Explicit vs. Implicit Trust Anchors terminology
  - Clarifies the bootstrapping
- Path-prefix of "/.well-known/”
  - Well-Known URIs [RFC5785]

-06 (in works)

- MIME references weren't strictly followed
  - -05 wraps in an extra PEM header
  - draft-josefsson-pkix-textual-01 (Network Working Group, expired 1/18/2013) has some interesting work in this area
  - Avoiding the issue by dropping all PEM headers and properly following the MIME types
  - Thanks to David Grant for pointing this out
- Server-side Key Generation
  - Additional protection of the response has been requested
- I hesitate to say anything; but we're pushing this one out faster

Implementation Highlights

- Thanks to Dan Harkins for performing interop testing between our implementations
  - I'd failed to implement persistent connections correctly
- Betting alignment w/ defined MIME types means slight parser changes (in progress)

- END