Status Quo

- RFC4880 & crypto-refresh quite vague on the semantics
- by design, some say
- but, is a signature valid?
Messages

- Guidance about reasonable resource limits on ABNF depth #114
- Describe how reply-to-all should work in the e-mail context #78
- Guidance on dealing with malformed packets in a stream #69
- clarification about whitespace #11
Certificates

- Should we mandate that cert components are unique? What about signatures? #129
- Certification-capable subkeys #123
- disambiguating conflicting preference subpackets in a cert #103
- certificate canonicalization #100
- Specify when a signature or key should be rejected #97
- Deprecate the use of "Key Expiration Time" packets (type 9) in V5 sigs #71
- Lacking guidance on merging secret keys #70
- Facilitate primary key rotation when revoking keys #64
- domain-specific trust constraints #12
- attestation signatures #10
- when is a certificate valid?
- revocations
  - hard: can never be undone (key material compromised)
  - soft: can be undone (key/user id retired)
- what to do with multiple encryption subkeys?
Signatures

- when is a signature valid? see this essay
  - does the cert have to be valid? now or at the signature creation time?
- subpackets
  - lack of clarity about semantics of subpackets in Direct Key Signatures #170
  - Intended Recipient Fingerprint subpacket interaction with other security indicators #169
  - what does criticality mean for "Key Flags" and "Features" subpackets? #155
  - Clean up description of Key Flags subpacket #120
  - Trust Signature description unclear #116
  - Specify which subpackets can be in the unhashed region #96
  - how many do we expect, what happens if there are more?
  - key flags should be mandatory on subkey bindings
  - reason for revocation should be mandatory for revocation sigs
  - better way to scope trust signatures
  - a tsig depth of 255 should mean infinite, not 255