Currently at -03 revision

Updates since Seoul include

- added TLS 1.3 support
- added section on raw public keys
- softened language on record order
- updated discussion ofUKS attack
- edits for language and consistency

Fairly well-cooked with respect to TLS considerations
TBD before wglc

- Need to add pseudocode and test vectors
- Need to add edits based on Viktor’s most recent comments
- We know there may be additional DNS-related issues lurking in the background, need feedback from dnsop, dane, and dpriv working groups