DANE for S/MIME

Paul Hoffman

IETF 84, Vancouver

v01

Comparing S/MIME and TLS

- S/MIME is store-and-forward, not real-time
- Certificates are not required, but are very common
- There's also CMS, which is S/MIME without the assumption of mailing
- S/MIME root piles are usually (but not always) smaller than TLS root piles
- TLS is more widely implemented

The one main difference for S/MIME

- The domain name for lookup includes the left-hand side of the email address, encoded in Base32
- Using Base32 lets you encode lots of odd bits that can appear in LHSs, such as periods and non-ASCII characters
- Put the _smimecert next to the domain name so that the entire S/MIME namespace can be delegated
- “chris@example.com” is looked up as “MNUHE2LT._smimecert.example.com”

What should be in the doc?

1. Copy whole DANE-for-TLS RFC and make needed changes
2. Copy structure of DANE-for-TLS RFC and point to it but don't copy much
3. Say "we assume you read and understood DANE-for-TLS, and here are the relevant differences"