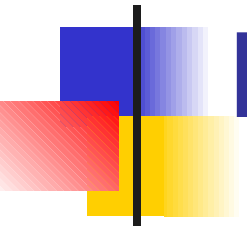
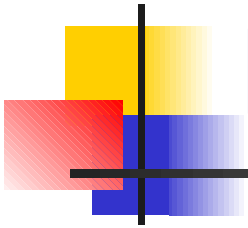


PKINIT20

Brian Tung

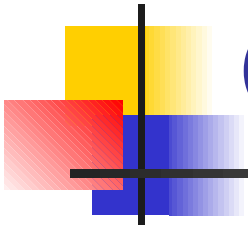
brian@isi.edu

Issues List by Jeff Hutzelman



Major Issues

- OPEN 013 – OCSP and optional revocation information
  - Merge spec into PKINIT or submit as separate draft?
- OPEN 017 - DH key derivation
- OPEN 031 - Which encoding - DER vs BER? (Love #2)
  - DER would be consistent, but some objects could be BER?
- OPEN 035 – Wrap CMS objects in OCTET STRINGs?
  - Change to on-the-wire protocol?
    - Does using IMPLICIT OCTET STRING avoid this?

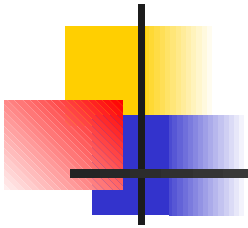


Questions

- OPEN 020 - Unauthenticated plaintext issues
- OPEN 028 - Nonce type?
  - Does this have to do with recommended sizes for nonce?
  - Check for consistency with clarifications?
- XXXX 030 - What key should the reply be enveloped with in the encKey case? (Love #1)
- OPEN 034 - subjectAltName/OtherName issues (Love #7)
  - Changed again with PKINIT20

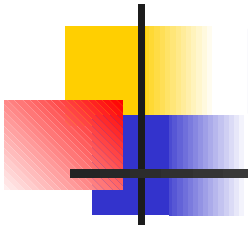
More Questions

- NEW 038 - DH groups selection
  - Move from RFC 2409 groups 1/2 to RFC 3526
- OPEN 039 - Root CA cert in chain?
- OPEN 040 - encryption certificate change not protected
  - Does this refer to removing legacy text?



Editorial

- DONE 002 - REMOVE use of raw public keys
- XXXX 004 - Security of cached DH values and use of a nonce
  - Zero nonce OK?
- XXXX 005 - Confirm alignment with CMS
- OPEN 007 - Confirm alignment with clarifications
  - What remains?
- OPEN 009 - Update PA types



More Editorial

- OPEN 021 - TrustedCAs context tags broken (Love #5)
  - Does anything remain?
- OPEN 024 - cname mapping proposal
  - Did Larry submit a mapping proposal?
- OPEN 026 - Unconstrained Integers (Love #6)
  - Is this related to nonce type issue? (028)
- NEW 037 - ASN.1 module inconsistency