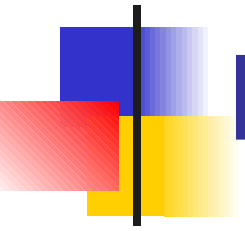


pk-init-21.txt

Brian Tung

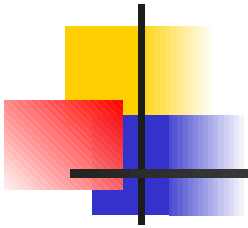
brian@isi.edu

Issues Believed Closed

- 499 (007): Refs1510bis – Clarifications
- 513 (021): Context tag inconsistency in TrustedCAs
- 518 (026): Unconstrained integers
- 523 (031): DER vs BER
- 527 (035): Wrap CMS objects in OCTET STRINGs

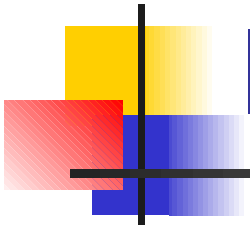
Issues Believed Closed (cont)

- 529 (037): ASN.1 inconsistency (*)
- 530 (038): Diffie-Hellman group selection (*)
- 531 (039): Don’t include root CA cert
- 612: AES algorithm OID (*)
- 666: Remove encryption cert text
- 667: Add RFC 2119 reference



Issues Believed Open

- 507 (015): PKINIT support
- 512 (020): Unauthenticated plaintext
- 516 (024): Mapping of cname
- 522 (030): Text for key to use in encKey case
- 526 (034): SubjectAltName/OtherName



Issues Believed in Limbo

- 501 (009): PA types
  - Awaiting completion of draft
- 509 (017): Diffie-Hellman key derivation
  - Extraneous text to be removed
  - Sam's comment later retracted?
- 611: Checksum issues
  - Ken's draft referenced in pk-init-21.txt
  - Review Ken and Sam's proposed approach