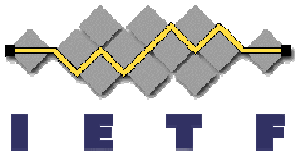
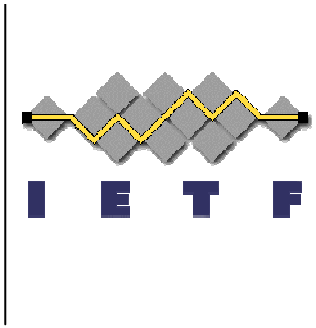
RFC 2716bis

Monday November 6, 2006



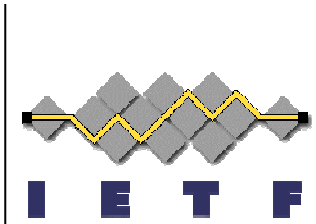
Draft-simon-emu-rfc2716bis-04.txt
Dan Simon
Bernard Aboba
IETF 67, San Diego, California

Document Status



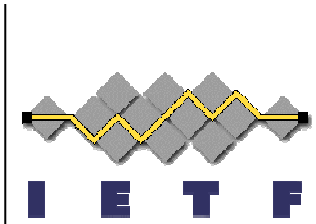
- Changes from RFC 2716
  - -04
    - Section 2.4: Clarified relationship of Peer-Id and Identity Response.
    - Section 4.2: Expanded discussion on certificate usage
    - Section 4.2: Added discussion of Peer-Id and Server-Id
    - Section 5.1: Added normative reference to RFC 3280.
  - -03
    - Section 2.2: Clarified retransmission responsibility (authenticator, not server).
    - Section 2.6: Clarified ciphersuite support requirements
    - Section 2.7: (Optional) privacy support.
    - Appendix A: Changes from RFC 2716.

Document Status (cont'd)



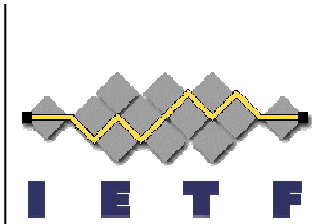
- Changes from RFC 2716
  - -02
    - Section 2.5: Added EAP-TLS key hierarchy diagram, EMSK formula corrected (no longer broken into halves), added definition of Session-Id, clarified that PRF in [RFC4346] is used (e.g. not version specific).
    - Section 2.6:Added mandatory-to-implement ciphersuites.
    - Section 4.6: Added section on packet modification attacks.
    - Changed TLS protocol references to [RFC4346] from [RFC2246], added reference to [RFC3280].
  - -01
    - Section 2.5: Addition of key derivation formulas from Key Framework Appendix
    - Section 4.1: Security claims
    - Section 4.3: Certificate usage restrictions

Document Status (cont'd)



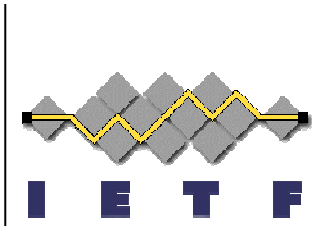
- Changes from RFC 2716
  - -00
    - Broadening of PPP-specific focus
    - Reference Update (Normative vs. Informative)
    - Section 2.4: Update of Identity Verification based on RFC 3748 advice (e.g. EAP-Identity/Response used only for routing).
    - Section 2.6: Removal of lower layer ciphersuite and compression negotiation via TLS

Open Issues



- From Joe
  - EKU of ANY?
  - What if there is more than one altSubjectName? Does order matter?
- Is the EAP-TLS certificate profile different from the TLS certificate profile?
  - RFC 4334 seems to assume it is.
  - However, implementations typically rely on TLS for certificate handling.

Next Steps



- Close remaining open issues, submit -05.
- Ready for WG Last Call?

Feedback?