draft-ietf-lamps-cms-aes-gmac-alg and
draft-ietf-lamps-crmf-update-algs

Russ Housley

IETF 110
LAMPS WG
draft-ietf-lamps-cms-aes-gmac-alg

• Provides OIDs and parameters for AES-GMAC
• IESG Evaluation raised a few comments:
  – Make RFC 5912 a normative reference
  – Expand Security Considerations
• With these changes, it is approved by the IESG
• Allows PBMAC1 [RFC8018] as an alternative for a password-based MAC
• For id-PasswordBasedMAC:
  – Transition the “owf” from SHA-1 to SHA-256
  – Modernize guidance on “iterationCount”
• MAC algorithms:
  – MUST support HMAC-SHA256
  – SHOULD support AES-GMAC with 128-bit key
• IETF Last Call is underway