draft-housley-lamps-crmf-update-algs

Russ Housley

IETF 109
LAMPS WG
Goal

• Update the cryptographic algorithm requirements for the Password-Based MAC in CRMF [RFC4211]

• The problem was discovered by Hendrik when he was working on updates to CMP [RFC4210]
Section 4.4 of [RFC4211]

• Password-Based MAC relies on a one-way function to compute a symmetric key from the password and a MAC algorithm

• All implementations …
  – MUST support SHA-1
  – MUST support HMAC-SHA1
  – SHOULD support DES-MAC and Triple-DES-MAC

• Update these to use modern cryptography
Proposed Replacements

• All implementations …
  – MUST support SHA-256
  – MUST support HMAC-SHA256
  – SHOULD support AES-GMAC with a 128 bit key
Way Forward

• WG Adoption, then immediate WG Last Call

• Of course, Tim will make all consensus calls for this document