draft-housley-lamps-cms-aes-mac-alg

Russ Housley

IETF 109
LAMPS WG

Goal

- slides-draft-housley-lamps-crmf-update-algs proposes that AES-GMAC be used as the SHOULD implement algorithm, but no algorithm identifier had been assigned
- Now, there is one. Thanks to NIST!
- Simple document to provide the object identifier and the needed parameters

GMAC OIDs

aes OBJECT IDENTIFIER ::= { joint-iso-itu-t(2)
country(16) us(840) organization(1) gov(101)
csor(3) nistAlgorithm(4) 1 }

id-aes128-GMAC OBJECT IDENTIFIER ::= { aes 9 }

id-aes192-GMAC OBJECT IDENTIFIER ::= { aes 29 }

id-aes256-GMAC OBJECT IDENTIFIER ::= { aes 49 }

GMAC Parameters

```
GMACParameters ::= SEQUENCE {
        nonce       OCTET STRING,
                    -- recommended size is 12 octets
        length      MACLength DEFAULT 12 }

MACLength ::= INTEGER (12 | 13 | 14 | 15 | 16)
```

Way Forward

- WG Adoption, then immediate WG Last Call

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