Crypto Keytable

Tim Polk
Russ Housley
November 16, 2011
Status

• Document *appeared* ready for last call
  – Then someone tried to apply it to 802.1X; seemed to lack some required features
  – Issues raised with editors, confirmed with one of NIST’s 802 folks
  – Problems identified in context of 802.1X, but seemed to apply more generally

• Editors asked WG chair to defer Last Call so they could address the identified issues

• New draft submitted at deadline
  – draft-ietf-karp-crypto-key-table-02
How Peer Identifies a Key

• The -01 draft included the mandatory field PeerKeyID, a 16 bit Integer
  – But 802.1X uses a name for the key
• The -02 draft specifies two fields, PeerKeyID and KeyName
  – PeerKeyID is still a 16 bit Integer, but may also have the special value null
  – KeyName is a variable length text field, which may also have the special values unknown and null
Interfaces

• The -01 draft included the interface field
  – Reviewers felt the definition was unclear and might not be sufficient in virtual environments

• The -02 draft explicitly allows the interface field to specify virtual or physical interfaces
Information about the Protocol

• The -01 draft included the Protocol field
  – In the 802.1X space the protocol name is insufficient
  – Implementers needed a key management domain and a network identifier
• The -02 draft adds the ProtocolSpecificInfo field and a registry
  – The ProtocolSpecificInfo field is an opaque blob with any extra information
  – The protocol registry entry includes the protocol name, identifies the specification, and defines each of the fields in the ProtocolSpecificInfo field (if any)
KDFs and AlgorithmIDs

• Once we defined a registry for information about the protocol, we started thinking about other fields

• Concluded that KDFs and AlgorithmIDs should also have registries
  – Primarily of use to specification developers, since these values do not affect bits on the wire
Availability of Keys

• The -01 draft included two time fields, NotBefore and NotAfter
  – Ran Atkinson pointed out a mismatch between the keytable and OSPFv2
    • OSPFv2 specifies four time values: KeyStartAccept; KeyStartGenerate; KeyStopAccept; KeyStopGenerate

• The -02 draft includes four time fields:
  – SendNotBefore; SendNotAfter; RcvNotBefore; RcvNotAfter
Open Issues

• 802.1X folks suggested a need for lots of keys
  – NIST was rather conservative in its guidelines for AES-GCM, so they could envision a need to change keys frequently

• Editors meant to change the LocalKeyID field from 16 bit Integer to Integer
  – Restriction on number of local keys is unnecessary
Way Forward

• Editors to resubmit this week removing restriction on size of LocalKeyID

• Ask WG Chair to review
  – Last Call if chair believes new text is sufficiently mature