IPsecME WG 2012-03-26

More Raw Public Keys for IKEv2

Tero Kivinen <kivinen@iki.fi>
AuthenTec

draft-kivinen-ipsecme-oob-pubkey-00.txt

Current Status

- Current IKEv2 do support raw public keys, but only PKCS#1 encoded RSA keys
  - “Raw RSA Key” contains a PKCS #1 encoded RSA key, that is, a DER-encoded RSAPublicKey structure (see [RSA] and [PKCS1])
- Some internet of things kind of things want to use ECDSA etc types of keys instead of RSA keys as they are smaller

What is Added

- This draft adds:
  - New Certificate Encoding format
    - Carrying SubjectPublicKeyInfo structure of PKIX Certificate
      - This allows us to support whatever formats PKIX does
  - New Certificate Encoding type for that format
  - Specifies that in Certificate Request Payload Authority field MUST be empty if this type is used.
- Similar work has been done for TLS
  - draft-ietf-tls-oob-pubkey-02.txt

Questions to the IPsecME

- Should this be working group document?
  - I think it is not needed, we can work this as individual document instead
- Should this be Standard Track document?
  - I myself think Informational is good enough
- What should be done for the old Raw RSA public key format?
  - Deprecate it completely (make it MUST NOT)
  - Say SHOULD indicate both, SHOULD use and prefer new format if both are supported (current text)
  - Be silent (don't say anything)