# Raw Public Keys in IKEv2

AuthenTec Oy
Tero Kivinen
kivinen@iki.fi

draft-kivinen-ipsecme-oob-pubkey-02

# Motivations

- IKEv2 does support Raw RSA public keys, but in some environments implementors would like to use ECDSA keys, as they are smaller
  - IEEE 802.15.9, Internet of Things, LWIG
- ECDSA keys can be used with Certificates, but certificate support (code) is too big
- Pre-shared keys are not scalable
- Need a way to transport ECDSA keys in similar way than we already transport Raw RSA keys

# Description of Problem & Solution

- How to transmit any types of Raw Public keys over IKEv2
    - New Certificate Type
    - Reuses SubjectPublicKeyInfo object from X.509
        - Can support any public key type that X.509 supports now or will support in future
- Now we have two ways to transport Raw RSA public keys

# What to Do with Raw RSA Public Key Type

- Make this new format completely optional
  - Leave old as is, both can be used, this document can be informational, does not need to updated RFC5996
- Make this recommended, but keep old
  - Leave old as is, but make this format as preferred (SHOULD for this and SHOULD NOT for old format), this document should be standard track, and update RFC5996
- Obsolete old format
  - Make old format as MUST NOT, and officially obsolete it, all implementations should switch to new format as soon as possible, this document must be standard track, and update RFC5996