NULL Authentication in IKEv2

draft-smyslov-ipsecme-ikev2-null-auth

Valery Smyslov
svan@elvis.ru

IETF 90

Examples of applicability

- Anonymous remote access to protected resources
  - user wants to preserve his/her anonymity, but at the same time wants to be sure that the resource is genuine

  One-way authentication: responder to initiator
- Communication with simple devices
  - user must be authenticated by device to be authorized to use it, but the device needs not always be authenticated

  One-way authentication: initiator to responder
- Opportunistic encryption
  - communication of the parties with no trust relationship

  Unauthenticated connection

Utilization

- AUTH Payload
  - is calculated by using pre-shared key syntax with SK_pi and SK_pr as the keys
    (identically to non-key-generating EAP methods)
- ID Payload
  - is present in the message to simplify parser
  - is ignored by receiver
  - is recommended to contain no data and to have ID Type = 0

Questions to WG

- Naming issue
  - NULL Authentication?
  - NONE Authentication?
  - ANON Authentication?
  - Something else?

- Early code point assignment?

Thanks

- Comments? Questions?
- Please review and send feedback to the author