NULL Authentication in IKEv2

draft-ietf-ipsecme-ikev2-null-auth-01

Valery Smyslov
svan@elvis.ru

IETF 91

Changes since adoption

- INITIAL_CONTACT handling is clarified
  - INITIAL_CONTACT must be ignored if NULL Authentication is in use
- Early Code Point assignment is requested

Open issues

- No formal security proof
  - one-way authentication is not well analyzed (however it is also true for the core IKEv2 property of mixing and matching auth methods)
- Channel binding
  - more an implementation issue than a protocol issue
- More security considerations are needed
  - feel free to provide them

Thanks

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