IKEV1 GRAVEYARD

IPsec, IETF 104
March, 2019

Paul Wouters, RHEL Security

draft-pwouters-ikev1-ipsec-graveyard

1. Tell people to stop using IKEv1
2. Mark IKEv1 era algorithms as deprecated in IANA for IKEv2/ESP
   - Need an RFC for the “deprecated” column at IANA

- Does not provide updated algorithm guidelines as in the RFC 8221 / 8247 series
- No other ponies (yes I would like to kill AH too)