IPsecME WG

Paul Hoffman, VPN Consortium
Yaron Sheffer, Porticor (remote)

IETF 89, London, March 2014

v2

Agenda

- Blue sheets, agenda bashing, note well
- Recent WG activity and inactivity
- IPsec in constrained environments
  - Overview -- Tero Kivinen
  - draft-mglt-dice-diet-esp -- Daniel Migault
  - draft-mglt-lwig-minimal-esp -- Daniel Migault
- New crypto algorithms and modes
  - draft-nir-ipsecme-chacha20-poly1305 -- Yoav Nir
- Opportunistic encryption using IPsec
  - draft-sheffer-autovpn -- Yoav Nir
  - Bootstrapping IPsec from DNS requests -- Paul Wouters
- IKEv2/IPsec context definition
  - draft-plmrs-ipsecme-ipsec-ikev2-context-definition -- Daniel Palomares
- Other stuff -- Remainder of time

Note Well

- You agreed to the Note Well about intellectual property rights (IPR) when you registered for this meeting
- You can see the Note Well text on your schedule
- If you haven't read it before now, you really should: it is important and you agreed to it

Recent WG activity

- IKEv2 fragmentation (draft-ietf-ipsecme-ikev2-fragmentation) just went into IETF Last Call
- Crypto requirements for AH and ESP (draft-ietf-ipsecme-esp-ah-reqts) just went into WG Last Call
- Signature authentication in IKEv2 (draft-kivinen-ipsecme-signature-auth) will go to IETF Last Call soon

Recent WG inactivity

- We were not able to get enough interest from the WG to get consensus on a single AD VPN proposal, even with a couple different attempts
- Almost all the interest was from the many authors of the three proposals
- We asked the authors if they wanted to combine their work, and heard nothing back
- Unless we hear otherwise by the end of the week, AD VPN work is dead in the WG, but it might happen as individual submissions