IPsecME Working Group
IETF 86, Orlando

Paul Hoffman
Yaron Sheffer

Where we are

- Hanging out waiting on AD to follow up on the auto-discovery VPN problem statement and send it to IETF Last call
- Have a few focused drafts that done-ish
- Once AD VPN problem statement is out of IETF Last Call, we want drafts of proposed solutions

Today's agenda (1 of 2)

- **Auto Discovery VPN Problem Statement and Requirements** - draft-ietf-ipsecme-ad-vpn-problem - 15 mins
- **A TCP transport for the Internet Key Exchange** - draft-ietf-ipsecme-ike-tcp - 20 mins
- **Additional Diffie-Hellman Tests for IKEv2** - draft-ietf-ipsecme-dh-checks - 5 mins
- **Signature Authentication in IKEv2** - draft-kivinen-ipsecme-signature-auth - 10 mins

Today's agenda (2 of 2)

- **More Raw Public Keys for IKEv2** - draft-kivinen-ipsecme-oob-pubkey - 5 mins
- **Cryptographic Algorithm Implementation Requirements and Usage Guidance for ESP and AH** - Not-quite-submitted draft - 15 mins
- **Gateway discovery and addressing** - draft-mglt-ipsecme-security-gateway-discovery and draft-mglt-ipsecme-alternate-outer-address - 5 mins
- **Simple VPN solution using Multi-point Security Association** - draft-yamaya-ipsecme-mpsa - 5 mins
- *If time permits*: draft-gundavelli-ipsecme-3gpp-ims-options - 5 mins

Next steps

- IETF LC for AD VPN PS
- WG last calls for some of the near-done documents
- Limited new work