# IPsecME WG
# IETF 92, Dallas

Yaron Sheffer
Paul Hoffman

# WG status report

- draft-kivinen-ipsecme-signature-auth was published as RFC 7427
- draft-ietf-ipsecme-ikev2-null-auth is done with WG review, -05 was issued yesterday, and Kathleen will move it to IETF Last Call if there are no more changes needed
- Current accepted work: draft-ietf-ipsecme-ddos-protection

# Agenda

- Chairs' view of draft-ietf-ipsecme-ddos-protection discussion history – 5 mins
- draft-ietf-ipsecme-ddos-protection discussion – 60 min
- draft-nir-ipsecme-chacha20-poly1305 call for adoption – 10 min
- draft-mglt-6lo-aes-implicit-iv, meant for 6lo WG – 5 min
- Other stuff – 5 min

# Discussion history of ddos-protection

- A lot of progress since Honolulu, but we’re not there yet
- Valery joined Yoav as co-author, draft is managed on GitHub
  - Discussion is strictly on the list!
- Changed the puzzle from hash to PRF
  - Had a discussion about performance and deterministic client behavior
  - With the current version client is free to choose hardness – too much logic?
- New version published with major improvements
  - Specifically around IKE_AUTH