IPsecME WG
IETF 79, Beijing

Paul Hoffman and Yaron Sheffer
Today

• Blue sheets
• Agenda-bashing self-reference
• Failure detection open issues – 45 min
• High availability protocol open issues – 45 min
• Other topics?
Before today

• RFCs published since Maastricht
  – RFC 5996, IKEv2bis
  – RFC 5998, mutual EAP authentication
  – RFC 6207, high-availability problem statement

• RFC to be published soonesque
  – Roadmap
After today

• Close out all the open issues on the HA protocol and failure detection drafts
• Create more open issues as appropriate
• Have a WG last call on each draft
• Take them to our AD for IETF-wide review
• Maybe add more work to the WG, or maybe shut down and leave the mailing list open
IKEv2 Reauthentication

- Reauthentication in RFC 5996 is IKE_SA_INIT, IKE_AUTH, CREATE_CHILD_SA * (n-1), where n is the number of children of the IKE SA to be reauthenticated.

- Problems:
  - Too many exchanges! n-1 additional round-trips is unnecessary overhead.
  - Exchange collision handling is unspecified, and is sometimes impossible because responder can't detect that the reauthentication is occurring.

- Possible solutions:
  - draft-welter-ipsecme-ikev2-reauth-00
  - Alternate proposal (IKE_AUTH on IKE SA to be reauthenticated) discussed on-list, new draft TBA.