Agenda

• WG status – 5 mins
  – draft-ietf-ipsecme-ad-vpn-problem
  – ECDSA design team
• http://www.ietf.org/proceedings/85/ipsecme.html
• WG document: draft-ietf-ipsecme-ike-tcp – 15 mins
• Non-WG documents (see next slide)
Non-WG topics for today

- draft-kivinen-ipsecme-oob-pubkey – 15 mins
- draft-mcgrew-ipsec-me-esp-ah-reqts – 15 mins
- draft-zhang-ipsecme-multi-path-ipsec – 15 mins
- draft-harkins-ikev3 and draft-kivinen-ipsecme-ikev2-minimal – 15 mins each
- draft-mglt-mif-security-requirements – 10 mins
- draft-gont-opsec-vpn-leakages – 10 mins
Current draft needs revision based on WG Last Call comments

May need more discussion after we see the revision

Then on the AD and to IETF Last Call
ECDSA design team

- Report was recently sent to the list
- We want more comments on it soon
- Report included the reasons why the specific proposal was made
- Will turn into an Internet-Draft for the WG