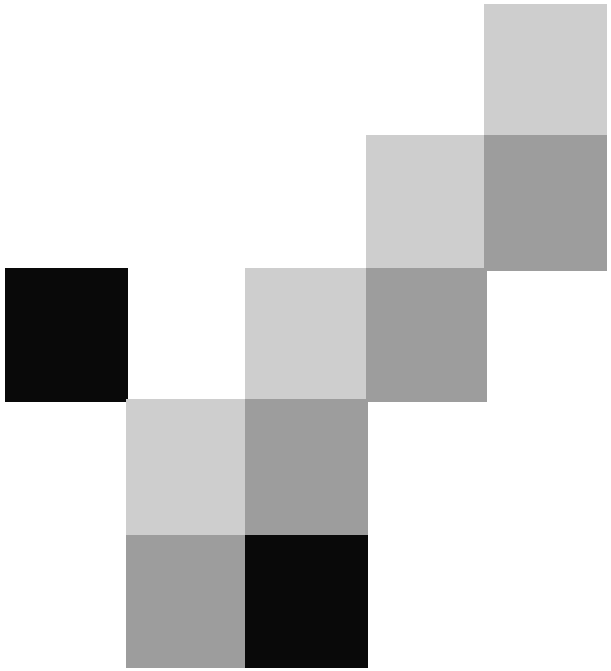

HMIPv6 Security – Next Steps

MIPSHOP WG, IETF 67

vijay.devarapalli@azairenet.com
smfaccin@marvell.com

HMIPv6 Security

- HMIPv6 (4140bis) assumes the use of IKEv2 between the MN and the MAP for security association setup
- Two authentication mechanisms are currently discussed
  - Certificates
  - EAP

Access Authentication based solutions

- Some of the current HMIPv6 security solutions are based on deriving keys from access authentication
- But if MN has credentials that it can use for access authentication, then it is straightforward to run EAP over IKEv2 with the MAP
- Proponents say it saves one round trip to the AAA
  - But it is only done once in a MAP domain, not on every handoff

HMIPv6 Security

- The use of EAP over IKEv2 is sufficient to progress HMIPv6 as a proposed standard
- Removes dependency on a separate standard solution for setting security between the MN and the MAP

Charter Item

- This does not mean we drop all work on HMIPv6 security
  - WG needs to decide if we still want to do another separate solution
- Experimental standards is an option if we decide to standardize one