# AAA-based Handover Keys Next Steps

MIPSHOP WG, IETF 69

Vijay Devarapalli (vijay.devarapalli@azairenet.com)

# Current status

- There is WG consensus to standardize a mechanism based on the AAA infrastructure to generate handover keys for FMIPv6
- No corresponding solution document adopted as a WG document

# Option #1

- Adopt draft-vidya-mipshop-handover-keys-aaa-04
- There was consensus early 2006 to adopt this document
  - But there was a delay in getting security reviews
  - Few other process related issues
- Need to test consensus again
- But authors have lost interest in this draft

# Option #2

- HOKEY-based solution
- Write a document in MIPSHOP WG that describes how to generate FMIPv6-specific handover keys from the USRK
- But this is only applicable when EAP is used for access authentication

# Option #3

- A simple mechanism based on deriving a FMIPv6-specific key from a shared key between the MN and the NAS
  - The shared key is EAP MSK
- draft-yegin-fmip-sa-00.txt
- Again applicable only when EAP is used for access authentication
  - Hints at using this mechanism for non-EAP environments, but not much detail

# Option #4

- Standardize nothing
  - It would be desirable to have someone wanting to use this
  - Remove AAA-based handover keys from the charter
- FMIPv6 can still progress to Proposed Standard based on draft-ietf-mipshop-handover-key