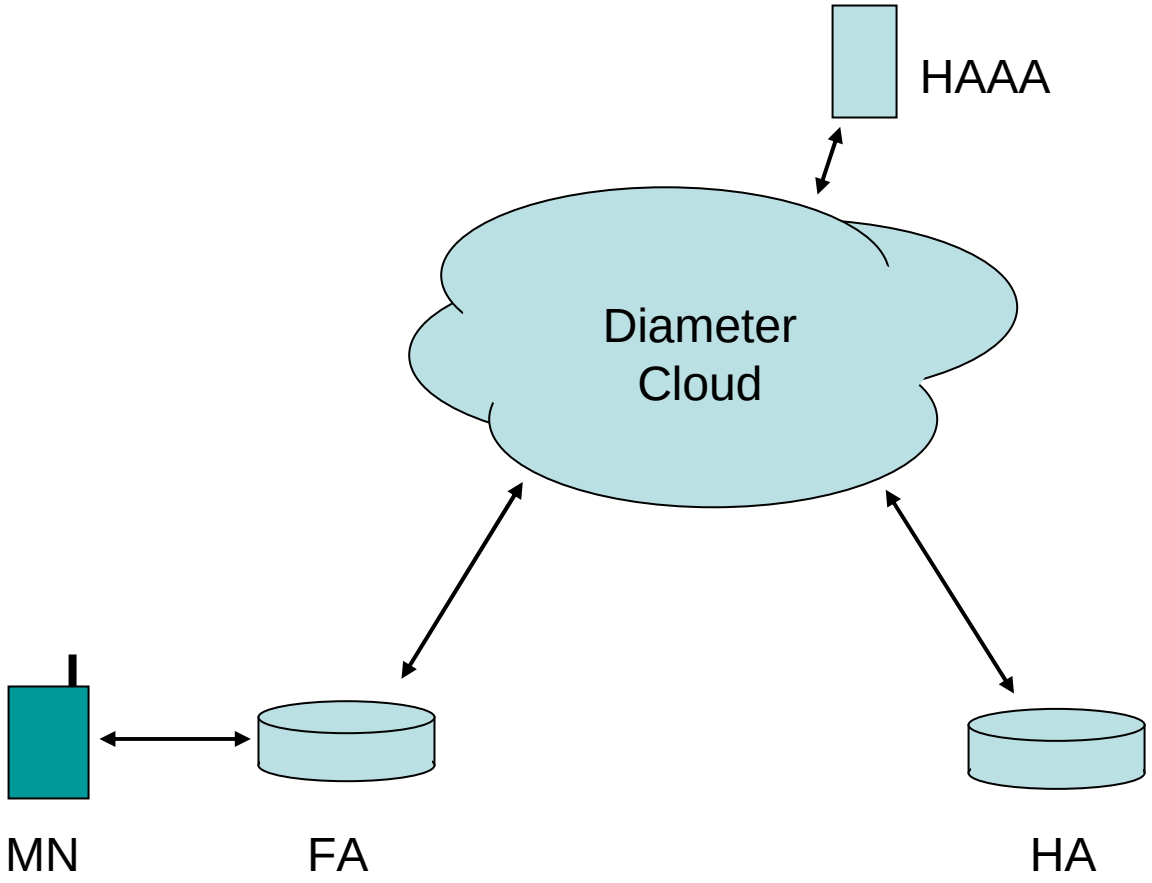
Diameter MIP4 Application, Present & Future

MIP4 WG, IETF 70

OUTLINE

- Existing RFC 4004 Architecture
- 3GPP2 and WiMAX Architecture
- Requested work
- Issues
- Next Steps

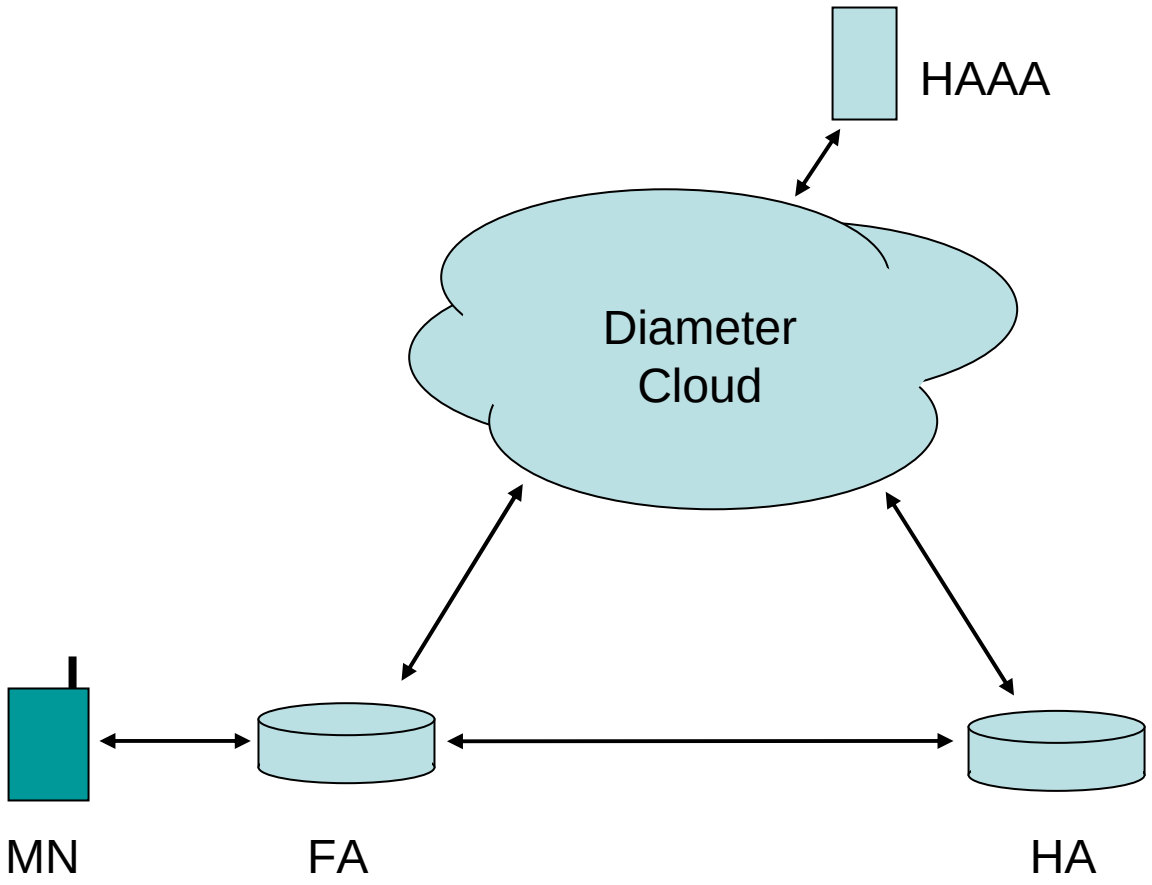
Diameter MIP4 Application (RFC4004)



RFC4004

- Initial RRQ included in AMR
  - MN might retransmit before RRP – performance issue?
- Designed to work with RFC 4721
  - MN-AAA Authentication extension
- Designed to work with RFC 3957
  - MN requests assignment of SAs in RRQ
  - MN includes its own choice of SPIs
  - FA and HA SPIs inserted into RRP
  - Authentication algorithm included in RRP
  - Replay protection mechanism included in RRP

3GPP2 and WiMAX



3GPP2 and WiMAX

- Run EAP for authentication
- Derive MN-FA & MN-HA keys from EAP MSK
- MN-FA & FA-HA Keys are pushed to the FA from Diameter cloud during EAP
- FA sends RRQ directly to HA
- HA retrieves MN-HA key from HAAA
- MN-AAA Auth Extension not used
  - 3GPP2: supported for legacy MNs
  - WiMAX: not supported

Requested Work

- A new Diameter MIP4 application
  - Support retrieval of keys from HA
  - No need to distribute FA keys
  - No need for MN-AAA auth extension (RFC 4721)
  - No need for MN-AAA-Keys (RFC 3957)
  - Send MIP4 RRQ directly from FA to HA
    Send MIP4 RRP directly from HA to FA

Issues

- How to configure MSA parameters such as SPIs and Algorithms?
  - Mobility Agents
  - MNs
- Does FA need to authenticate initial RRQ?
  - Current 3GPP2/WiMAX does access auth with EAP

Next Steps

- Need a draft outlining new architecture
- Need a plan for SPI-distribution and crypto-agility
- Discuss on mailing list