MEXT WG
IETF-71

Diameter MIP4 Application
AAA & Dynamic MSA Distribution

March 13th, 2008

Ahmad Muhanna

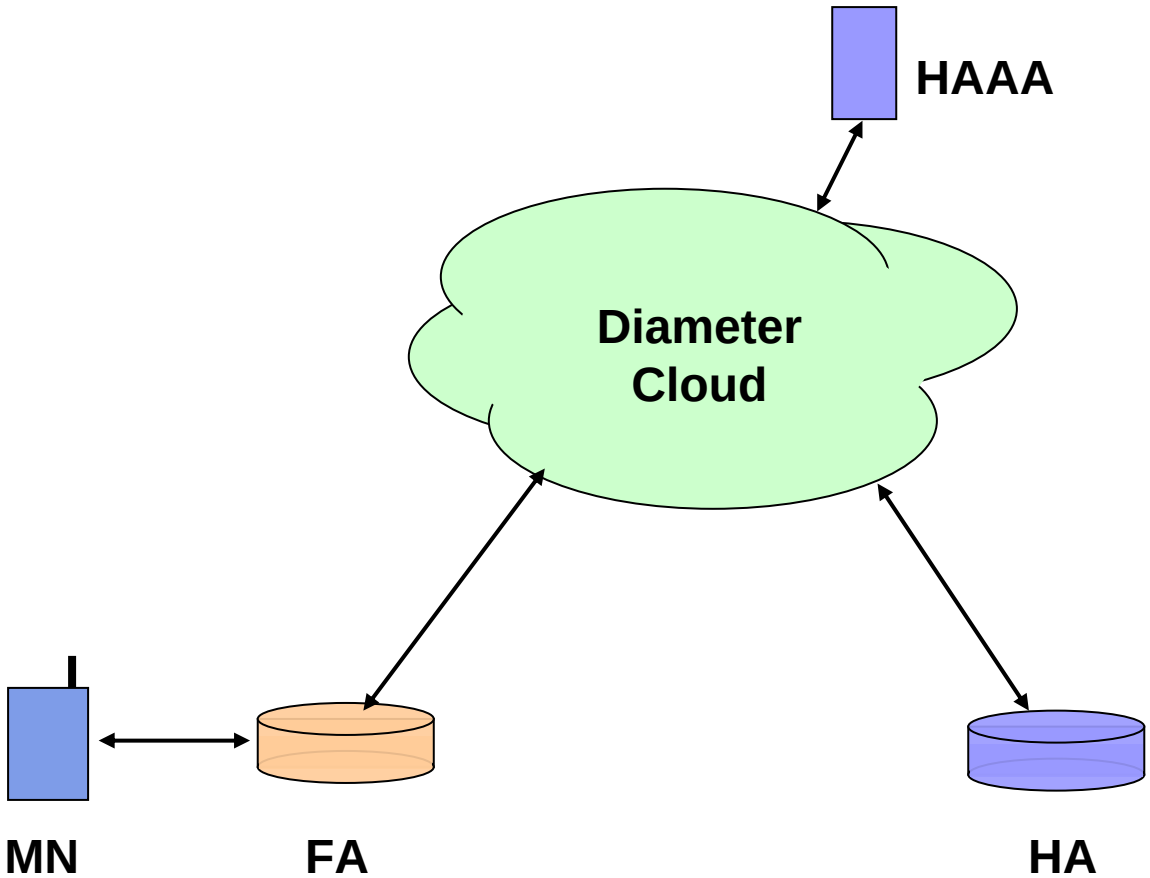
OUTLINE

- Diameter MIP4 Application Functionality
- Diameter MIP4 Application Auth & Authz
- Dynamic MIP4 MSA Parameters & Reqs
- Dynamic MIP4 MSA Allocation
  - RFC4004 Architecture
  - WiMAX Architecture
  - 3GPP2 Architecture
- What is Next?
  - What Diameter MIP4 Application Must Have
  - What WiMAX/3GPP2 Architectures are Missing

Diameter MIP4 Application Functionality

- User Authentication
- User MIP4 Authorization
- Dynamic MIP4 MSA Allocation and Distribution
  - MIP4 MN-HA MSA
  - MIP4 MN-FA MSA
  - MIP4 FA-HA MSA
- User Accounting

Diameter MIP4 Application (RFC4004)

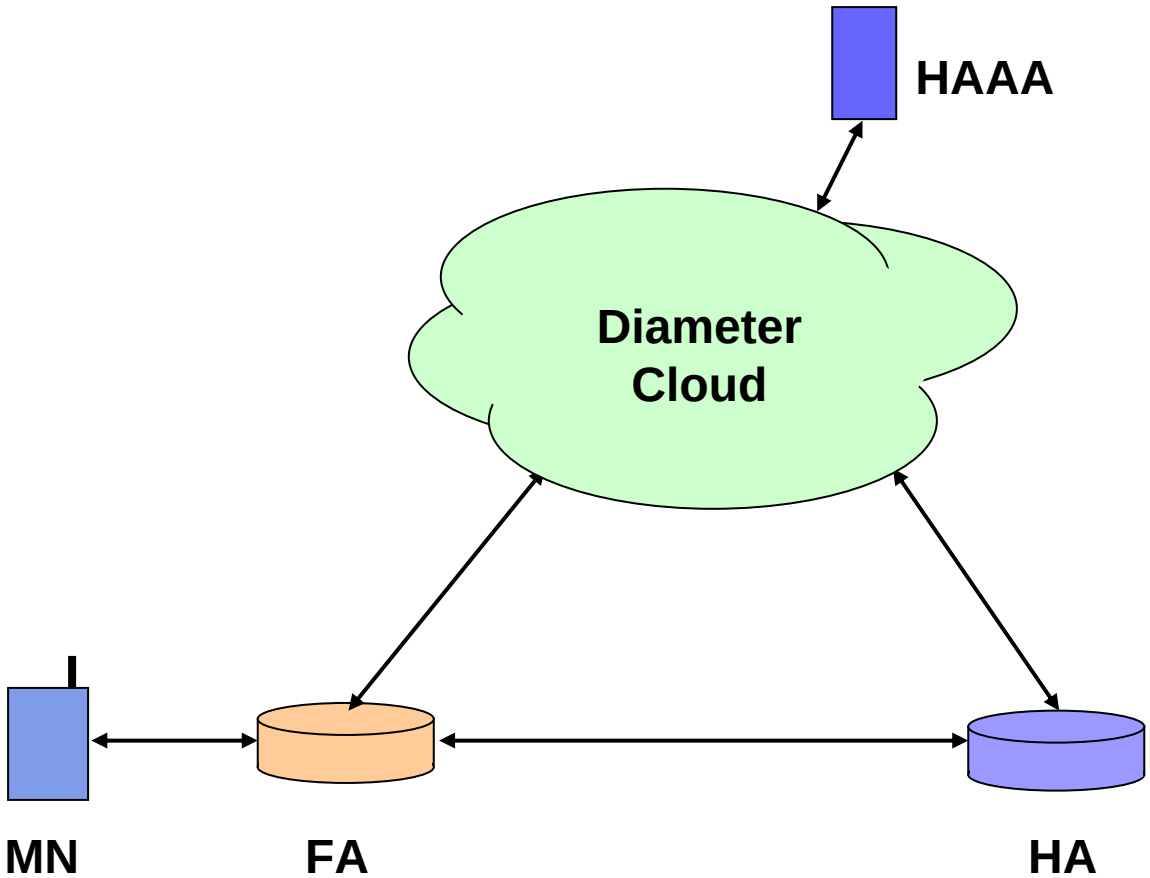


Diameter MIP4 Application Auth & Authz

RFC4004 Architecture

- Use of MN-AAA AE is Mandatory
- MN-AAA MSA is statically configured and indexed by MN NAI.
- MN-AAA AE SPI defines the used cryptographic Algorithm
- MIP4 signaling is coupled with Diameter AAA signaling.

WiMAX & 3GPP2 MIP4 Architecture



Diameter MIP4 Application Auth & Authz

3GPP2 Architecture:

- Use MN-AAA AE is Mandatory in Initial RRQ.
- MN-AAA MSA is allocated as a result of EAP Authentication.
- MN-AAA SPI is used to index MN-AAA MSA but no crypto agility.
- MIP4 signaling MUST be decoupled from Diameter AAA signaling

WiMAX Architecture:

- MN-AAA AE is **NOT** Supported
- MN-FA AE is Optional but possible to be mandatory.
- MN-FA MSA is allocated during EAP if MN-FA AE is Mandatory.
- No crypto agility is supported.
- HAAA delivers MN-HA key to HA based on trust relationship.
- MIP4 signaling MUST be decoupled from Diameter AAA signaling

Dynamic MIP4 MSA Parameters & Reqs

Dynamic MIP4 MSA Parameters

- Dynamic Secret Key, e.g. MN-HA key
- Security Parameter Index (SPI)
- Cryptographic Algorithm
- Replay Protection Mechanism
- Symmetric vs. Asymmetric SPIs
- Lifetime

Dynamic MIP4 MSA Allocation Requirements

- Cryptographic Agility
- Dynamic Replay Protection Negotiation
- Dynamic Keying and SPI

Dynamic MIP4 MSA Distribution

RFC4004 Architecture:

- Bootstrap MIP4 MSAs using MIP4 signaling.
- Use a statically configured MIP4 MN-AAA MSA (RFC4721) in initial RRQ to bootstrap other MIP4 MSA.
- Use RFC3957 for MIP4 MSA distribution.
- MN cryptographic capability & Algorithms is indexed against User subscription? Check?.
- MN's replay protection capability is indexed against User subscription. No issue!
- Assumes & Uses Asymmetric MIP4 MSA via asymmetric SPIs.

Dynamic MIP4 MSA Distribution

WiMAX Architecture:

- Use a statically configured EAP-AAA secret to bootstrap other MIP4 keys.
- Use EAP to derive EMSK, MIP-RK and then MN-HA, MN-FA keys.
- Use EAP to derive HA-RK and FA-HA keys.
- MN-HA SPI is dynamically derived at MN and AAA server separately per the MN NAI.
- MN-FA & FA-HA keys are delivered to FA during MN Access auth.
- MN-HA and possibly HA-RK Keys are delivered to HA during MN MIP4 Authorization via AAA **BUT** no MN-AAA AE is verified by the AAA server.
- HA use HA-RK to derive FA-HA key using a Hash function.
- No cryptographic agility mechanism is supported.
- No replay Protection Mechanism Negotiation, no issue.

Dynamic MIP4 MSA Distribution

3GPP2 Architecture:

- Use EAP with a statically configured EAP-AAA secret key to bootstrap other MIP4 keys.
- Use EAP to derive EMSK, CMIP4-MN-RK,
- From CMIP4-MN-RK the MN-AAA, and MN-AAA SPI are derived.
- From CMIP4-MN-RK the MN-HA, and MN-HA AE SPI are derived.
- MN-FA AE is NOT supported.
- FA-HA MSA is not generated as a result of EAP but through AAA.
- HAAA delivers MN-HA MSA after validating MN-AAA in initial RRQ.
- HAAA delivers FA-HA MSA based on a request from HA.
- No cryptographic agility mechanism is supported.
- No replay Protection Mechanism Negotiation

Diameter MIP4 Application Must Have

- Decouple MIP4 and Diameter Signaling.
- Allow MIP4 MSAs bootstrapping outside MIP4 signaling, e.g. during EAP.
- Allow FA-HAAA & HA-HAAA interfaces.
- Crypto Agility? i.e. real negotiation?
- Can HAAA delivers MN-HA MSA based on trust with HA ONLY?
- Scope of MN-HA SPI @ MN and HA?
- Does MN-NAI reflect the MN identity?

What WiMAX & 3GPP2 Must Have

- Is the use of MN-AAA AE Mandatory?
- Have a mechanism to allow Crypto Agility.
- Allow Asymmetric MIP4 MSA SPIs?
- No collision of dynamic MIP4 MSA SPIs.
- Replay Protection Negotiation. No Issue?
- Are multiple sessions per MN-NAI allowed?
- Is the user allowed to use the same NAI with Different MNs?
- Allow Dynamic MIP4 MSA lifetime

Questions & Comments?