MIPv6 bootstrapping with the Authentication Option protocol

MIP6 WG, IETF 66

Vijay Devarapalli, Alpesh Patel,
Kent Leung, Kuntal Chowdhury

Why?

- RFC 4285 is an alternative to IPsec (and IKEv2) for authenticating Mobile IPv6 signaling messages
  - Used in a couple of SDOs
- Current bootstrapping protocols focused on IKEv2. Work only when IKEv2 is used
- Developing bootstrapping mechanisms for RFC 4285 in the IETF is essential
  - Otherwise we end up with multiple proprietary mechanisms
  - Sometimes hackish solutions

What needs to be specified?

- Home address configuration
- Security association setup
- HA Discovery
  - Existing mechanisms can be used
    - DNS lookup
    - DHCP based assignment
    - DHAAD
- Reachability at the home address
  - DNS Update mechanism as described in draft-ietf-mip6-bootstrapping-split re-used

Home Address Configuration

- Mobile node sends a Binding Update with 0::0 home address
  - The MN MUST include the MN Identifier Option (RFC 4283)
- The Home Agent sends the home address in the Binding Ack
- Two new mobility options
  - Home Address Request Option
  - Assigned Home Address Option

Home Address Auto-configuration

- Currently only works for /64 home prefixes
- The MN sends the interface identifier in the lower 64 bits of the Home Address field in the Home Address option
- The Home Agent fills in the prefix and sends the home address back to the MN.

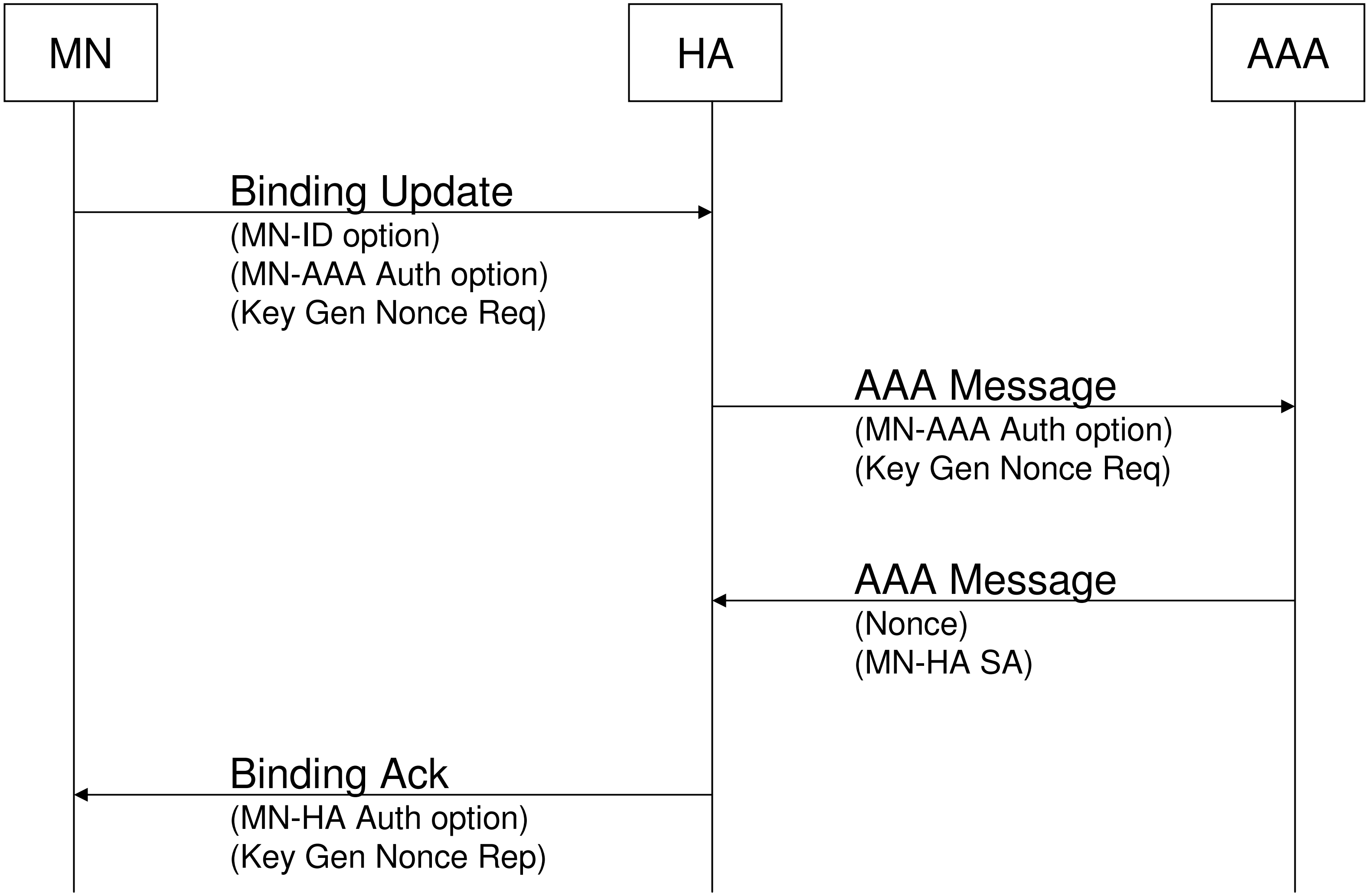
Security Association Setup

- RFC 3957-like mechanism for MIPv6

- An MN-HA SA is dynamically derived from the MN-AAA SA

- Assumptions
  - The MN depends on a AAA infrastructure for authentication and authorization
  - There is a long lived security association between the MN and the AAA (AAAH server)

Message flow for SA setup



MN

HA

AAA

Binding Update
(MN-ID option)
(MN-AAA Auth option)
(Key Gen Nonce Req)

AAA Message
(MN-AAA Auth option)
(Key Gen Nonce Req)

AAA Message
(Nonce)
(MN-HA SA)

Binding Ack
(MN-HA Auth option)
(Key Gen Nonce Rep)

What do we do?

- Do nothing
- Develop a solution in the IETF for bootstrapping the authentication option protocol
- Discourage the use of RFC 4285 for Mobile IPv6