HMIPv6 Security: Securing MN-MAP communication

draft-haddad-mipshop-hmipv6-security-02

MIPSHOP working group

IETF65

Why HMIPv6Sec?

- HMIPv6 does not specify any security mechanism between the MN and the MAP
- Need to establish this security association without any prior knowledge to be scalable
- Reuse existing security mechanisms where possible
- Add no additional signaling messages for the MN
- Charter item ;-)

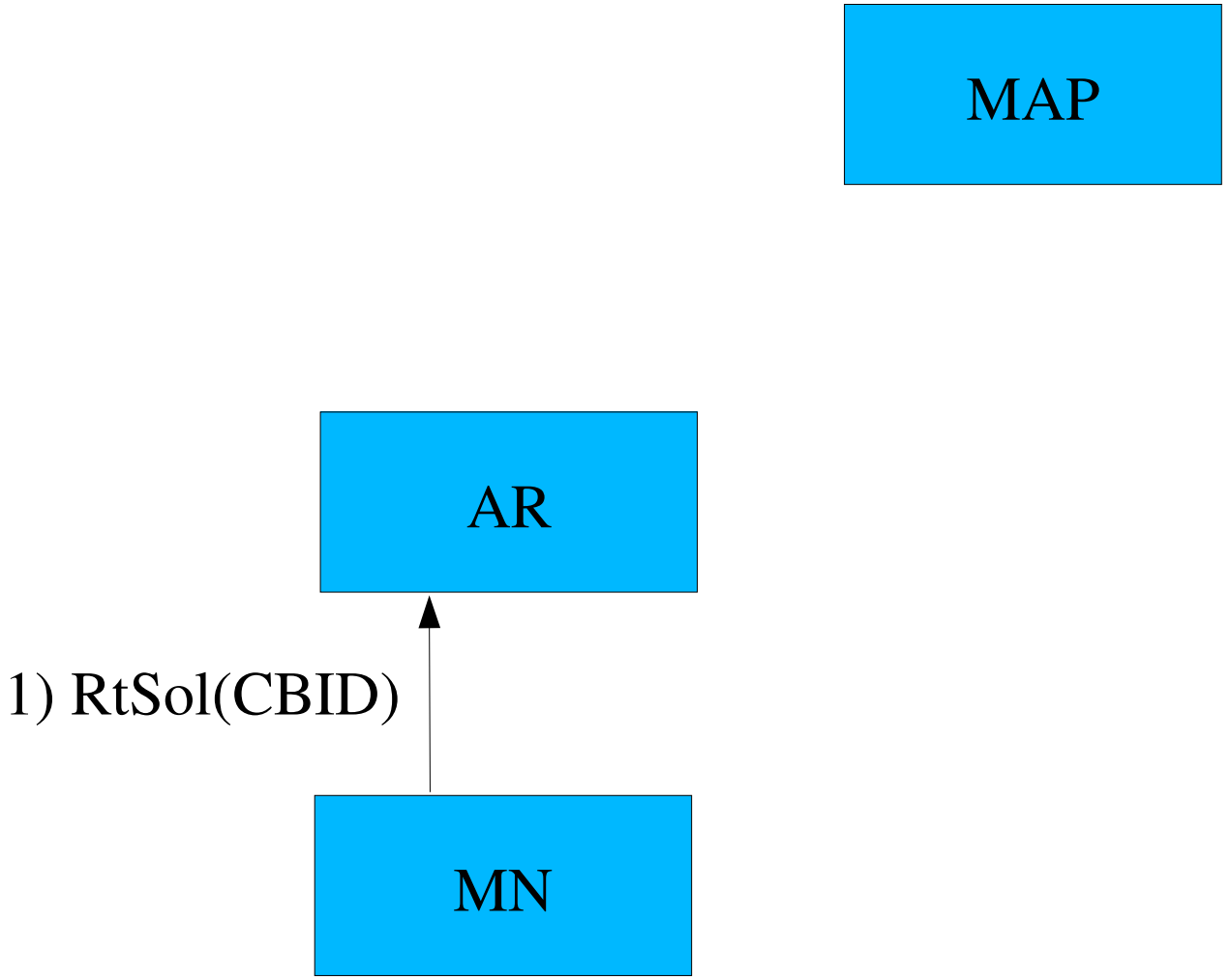
Assumptions

- MN uses Stateless Address Autoconfiguration (RFC2462) to generate the LCoA
- SEND will be deployed
- AR-MAP communication will be secured

Operation (1)

- The MN picks a 64 bit imprint IMP
- The MN generates a 128 bit CBID [HMAC-SHA1-128 (IMP,Kp)]
- The MN sends a SEND RS to the AR with the CBID. The RS also contains the MN's public key Kp. (CIO option)

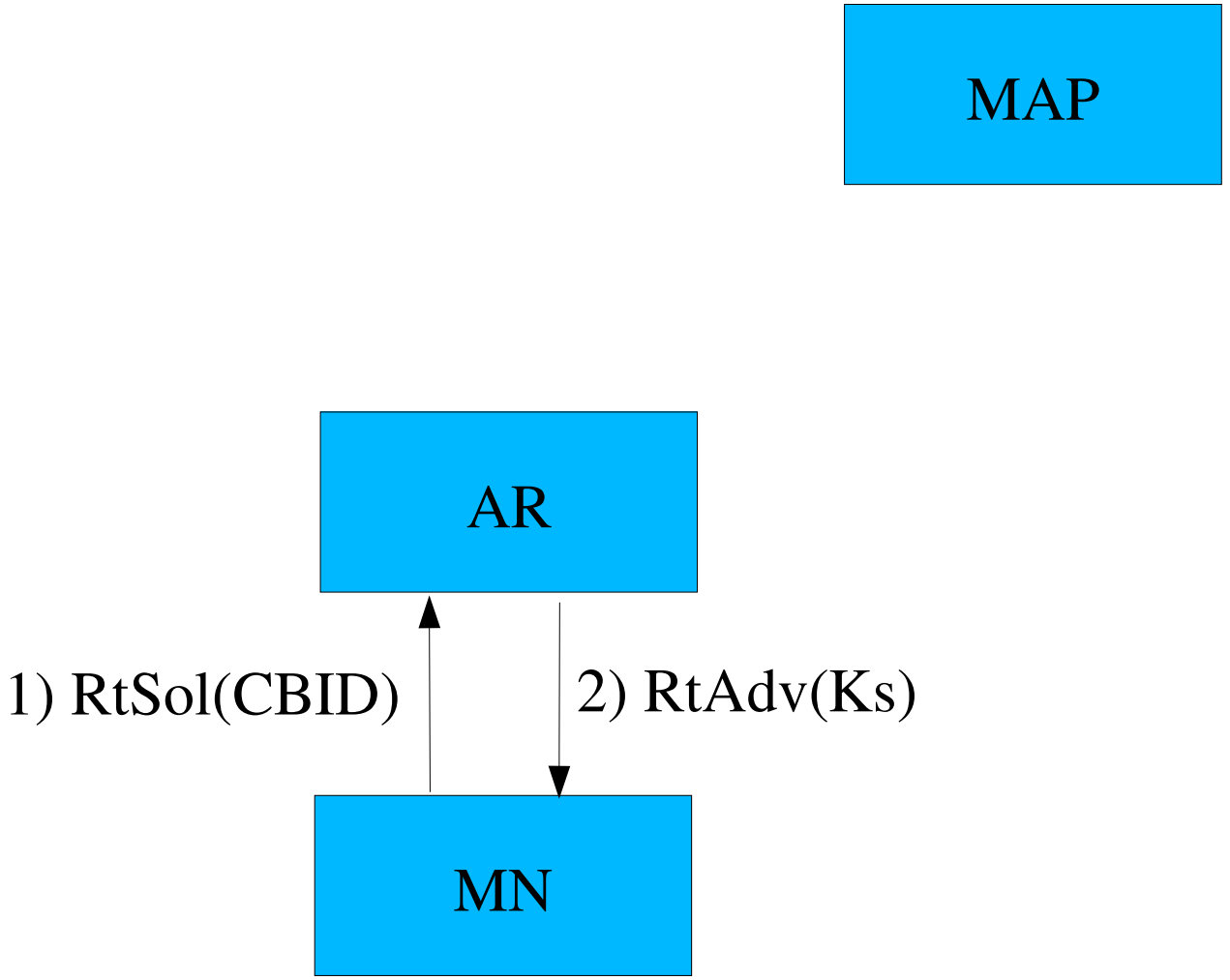
Operation (1)



Operation (2)

- The AR generates a secret key (Ks), encrypts it with Kp and sends it to the MN in the RA. (TPSK option)

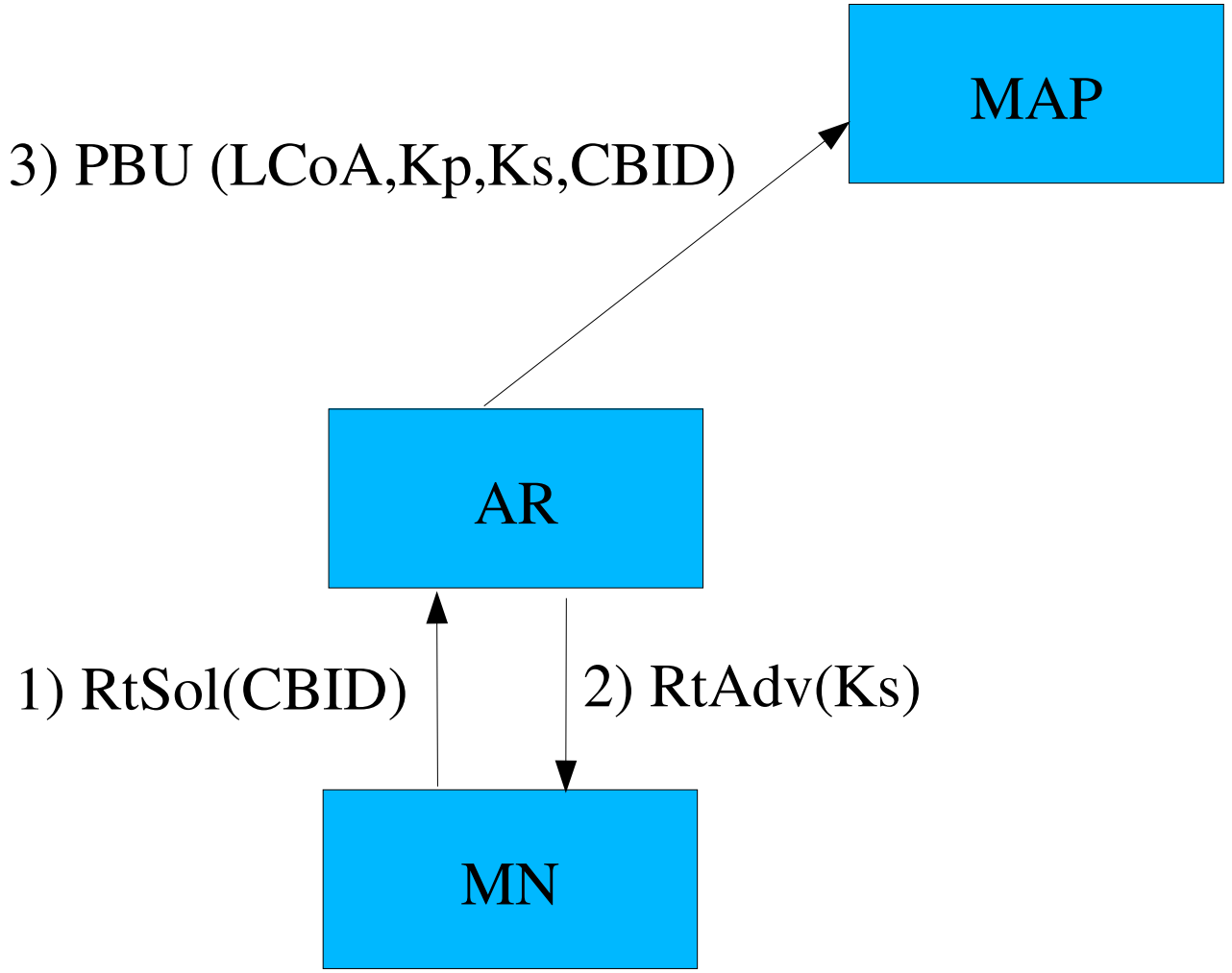
Operation (2)



Operation (3)

- The AR sends a PBU message to the MAP, which carries the MN's LCoA, Kp, Ks and CBID.
- After receiving the PBU, the MAP creates a BCE to the MN.

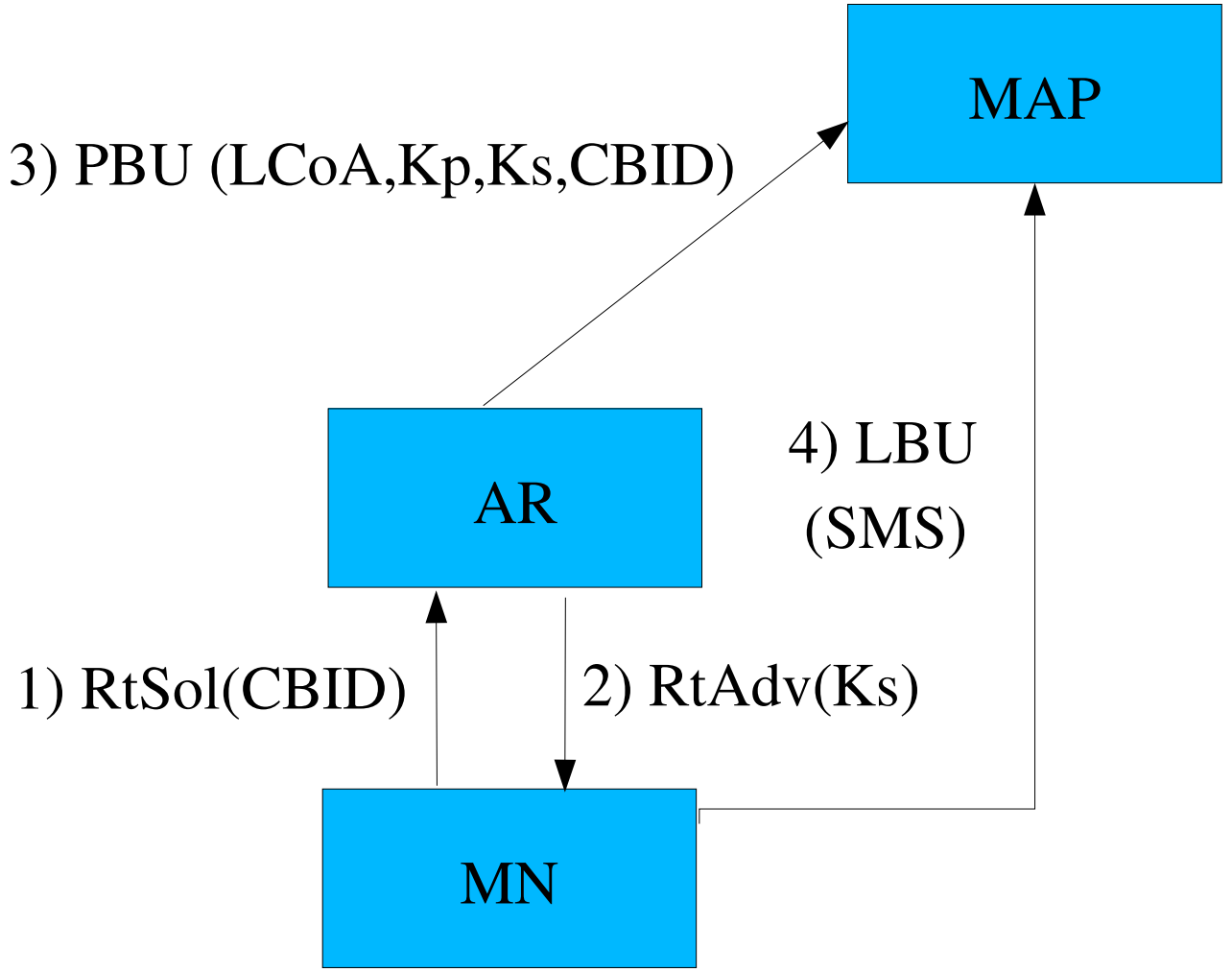
Operation (3)



Operation (4)

- The MN uses the IMP as the IID to auto-configure its RcoA.
- The MN initiates a Diffie-Hellman procedure and computes the public value X.
- The MN sends an LBU message to the MAP with the DH public value contained in a Session Mobility Secret (SMS) option.

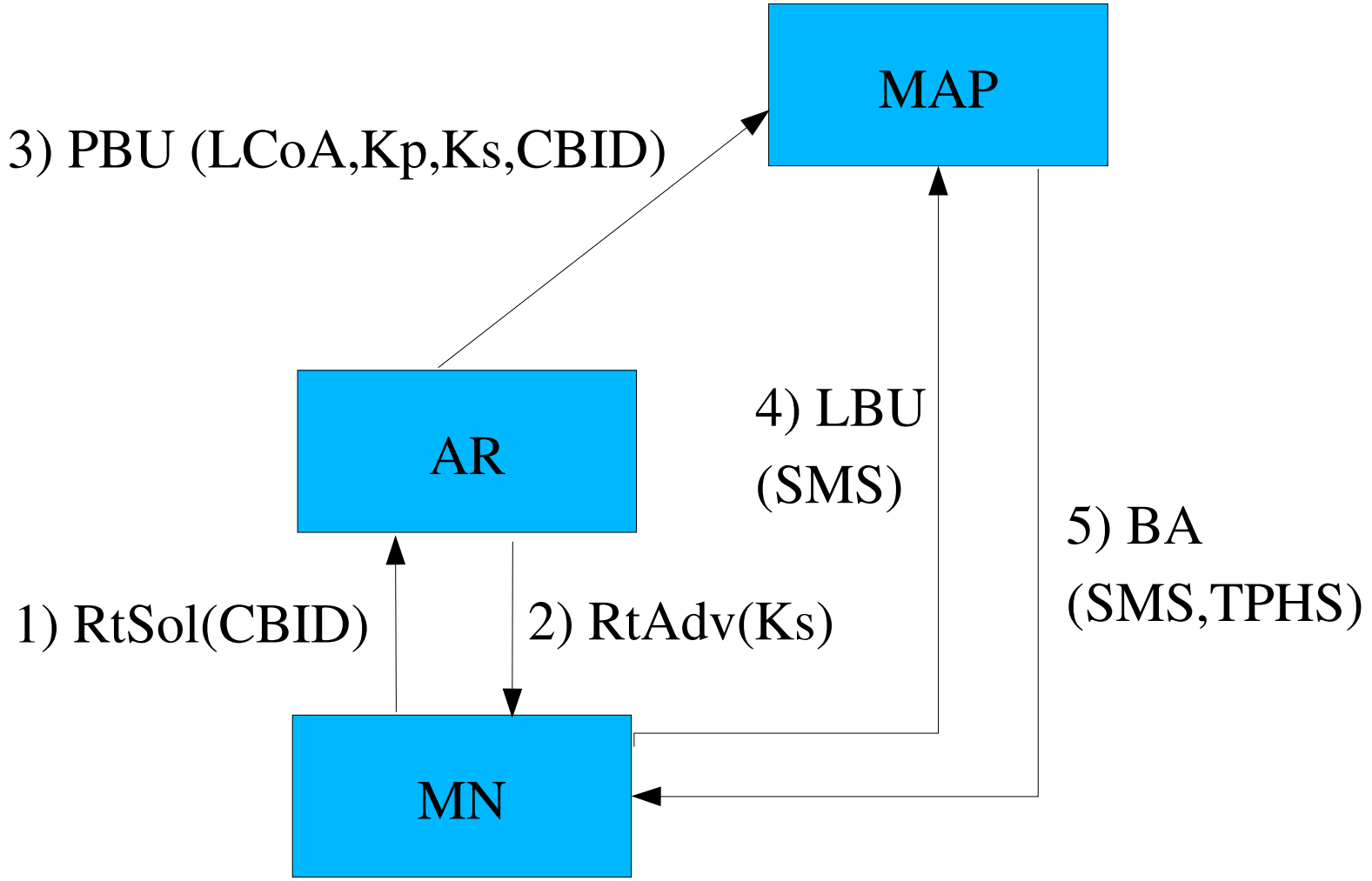
Operation (4)



Operation (5)

- The MAP checks the ownership of the RCoA and CBID by recomputing it from the RCoA's IID and the MN's public key (Kp).
- The MAP initiates a Diffie-Hellman procedure and computes the public value Y.
- The MAP sends an BA message to the MN with the DH public value Y contained in a Session Mobility Secret (SMS) option and the hash of the secret key Ks in the Third Party Hash Secret (TPHS) option.

Complete Operation



Advantages

- Simple
- Scalable
- No additional signaling messages on the MN-AR link (most likely a scarce resource)
- Resilience against DoS (partial integrity checks before full verification)
- No additional IPR issues

Further Action

- Is the WG interested in solving this problem?
- Does anybody see any technical problems with this solution?
- Adoption as a WG item

THANK YOU