Derivation, delivery and management of EAP based keys for handover and re-authentication

draft-ietf-hokey-key-mgm-00
IETF 69, July 2007

Madjid Nakhjiri
Yoshihiro Ohba

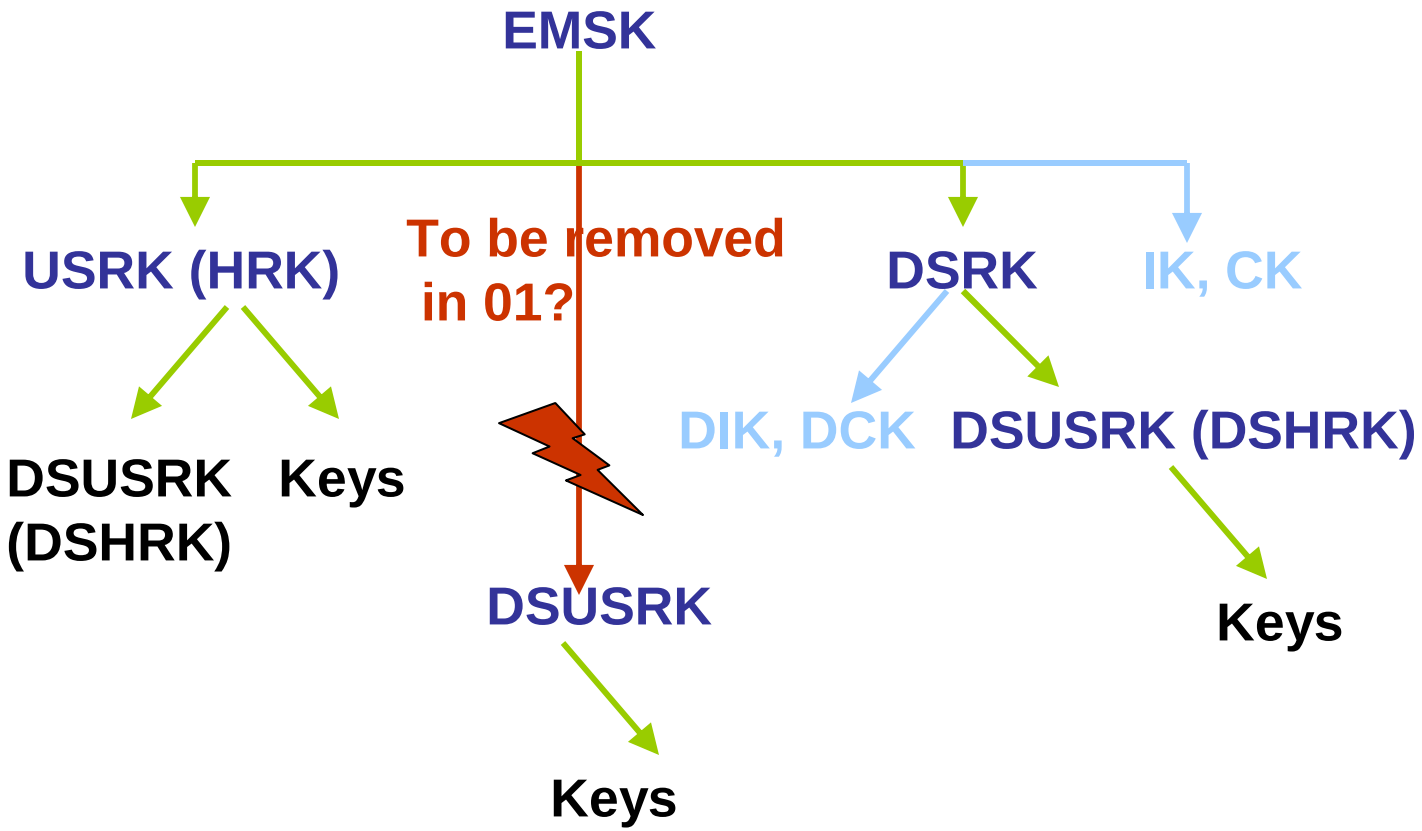
Contents

- EMSK based USRK (HOKEY) and DSRK derivation
  - Remove DSRK derivation (refer to emsk-hierarchy)?
  - Includes DSUSRK. To be removed??
- Generic Delivery Architecture (3 party)
- Generic Delivery Signaling (3 party)
- EMSK based keys for delivery protection
- USRK and DSRK based HOKEY hierarchies
  - Using [hokey-emsk-hierarchy]
  - DSHRKs
  - Delivery mechanisms for both.

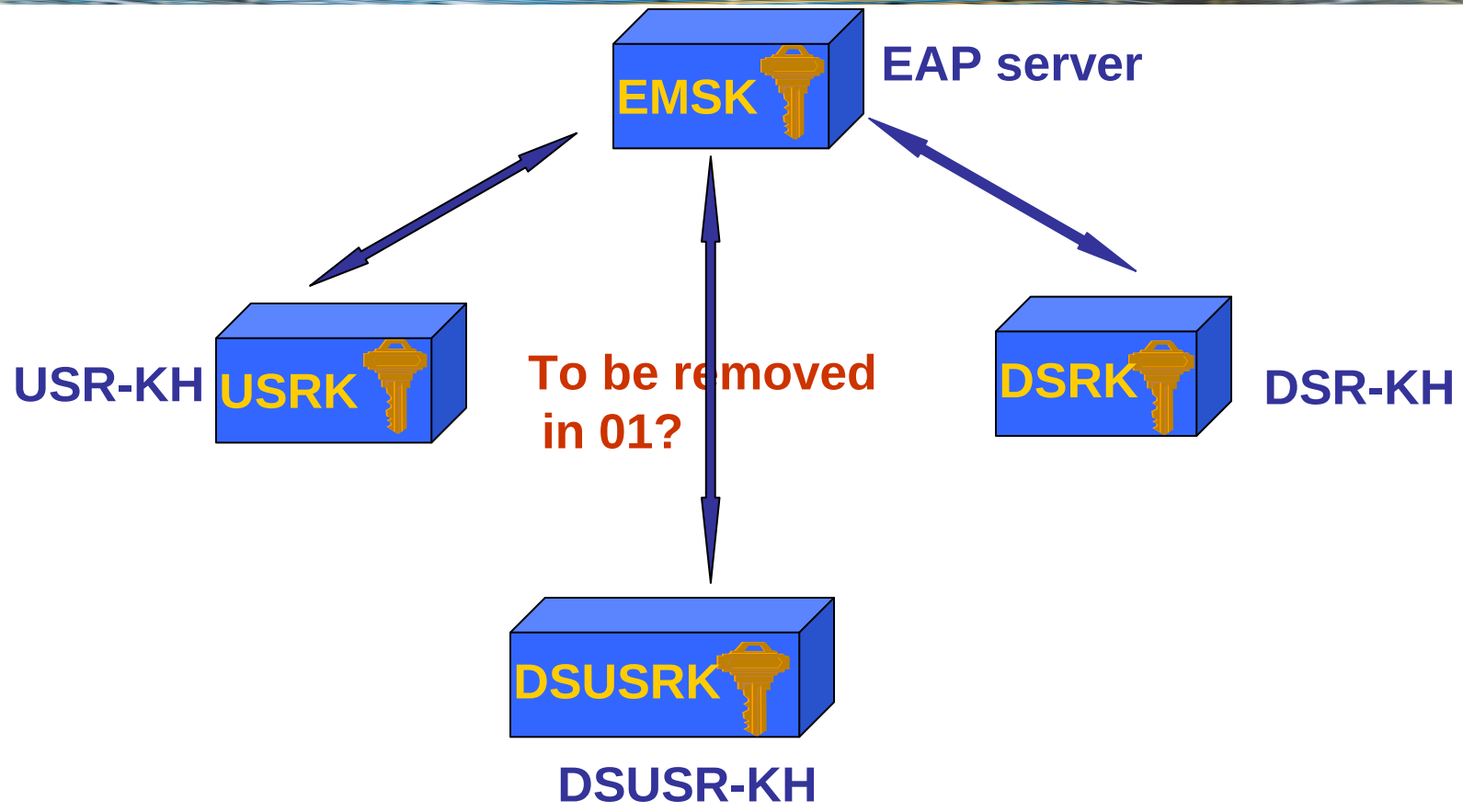
Hokey key hierarchy alternatives

- HOKEY Key hierarchy:
  - USRK based: EMSK->HRK->DHRK
    - Derive HRK, deliver to Hokey server (domain independent, or home), derive DSHRK for each domain Hokey server.
  - DSRK based: EMSK->DSRK->DHRK
    - Derive DSRK, deliver to domain AAA server, derive DSHRK for the domain, deliver to domain Hokey server.
  - DSUSRK based
    - Derive DSHRK from EMSK directly, deliver to domain HOKEY server (removed from Joe’s draft?)

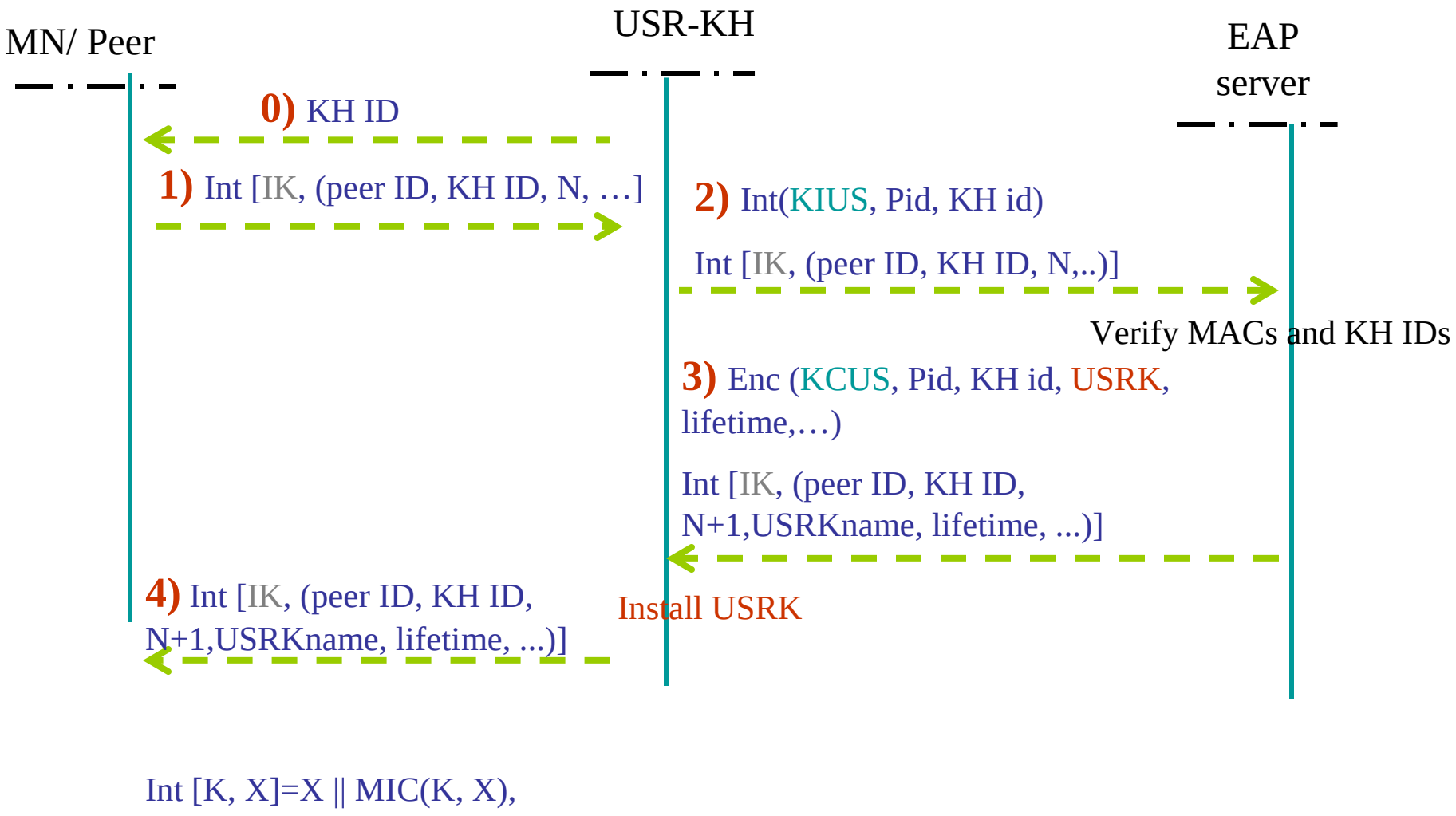
Key Hierarchy



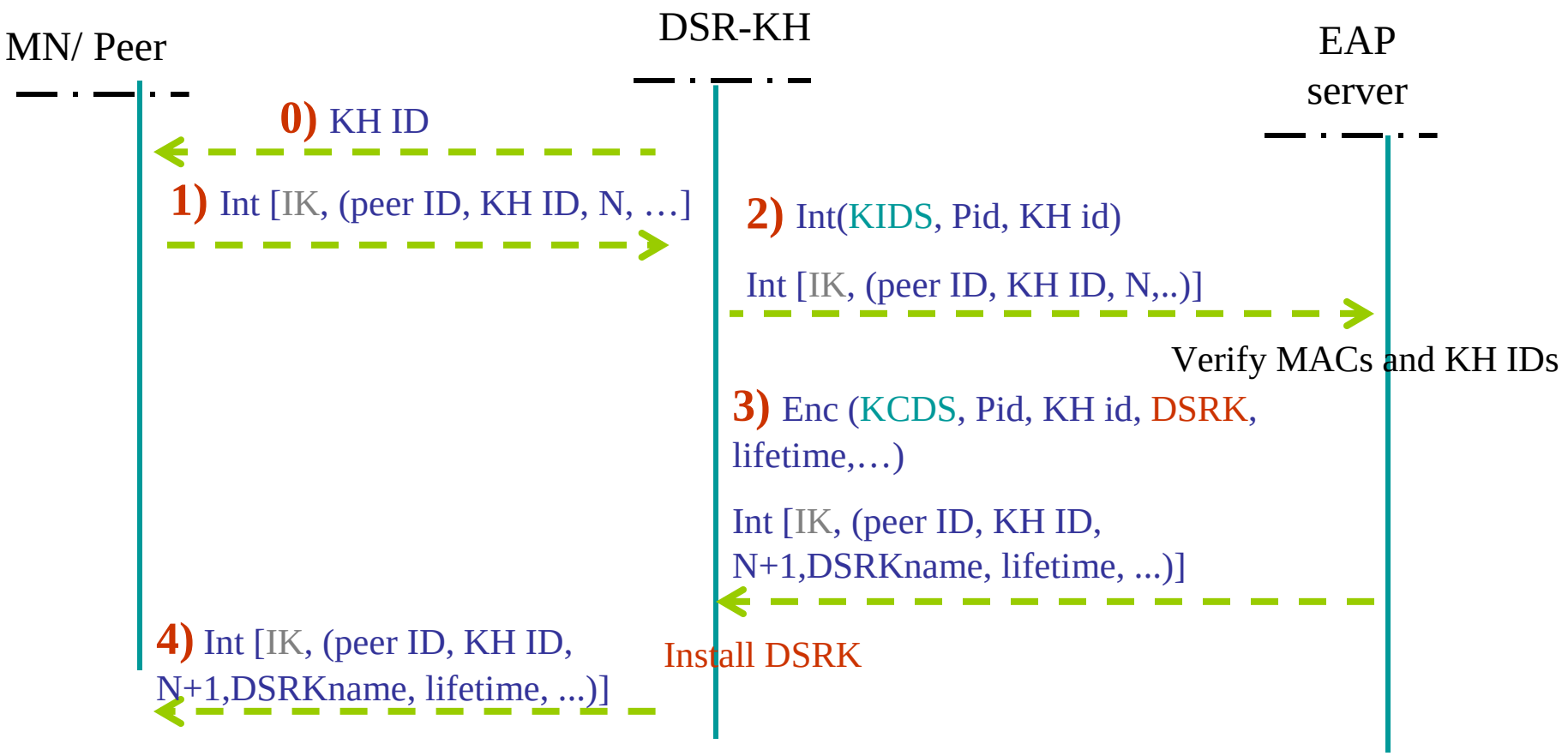
Key Delivery architecture



Delivery of USRK to USR-KH (HRK to HOKEY server)



Delivery of DSRK to DSR-KH



Yoshi’s comments

- Use nonce or time stamps for key exchange?
- Use server ID instead of domain ID? DSRK?
- Carry Key Type (USRK, DSRK, DSUSRK) along
- Carry one ID only, not both up and downlink ID

Future work/Issues

- Remove DSUSRK branch??
- Align key derivation details with hokey-emsk-hierarchy
  - Uses both usage and domain label (to fix)
- Derivation of keys at lower layers of hierarchy
  - Authenticator root keys