A keying Hierarchy for Managing Wireless Handover Security

draft-nakhjiri-hokey-hierarchy-03
IETF 67.5, Jan 2007

Madjid Nakhjiri

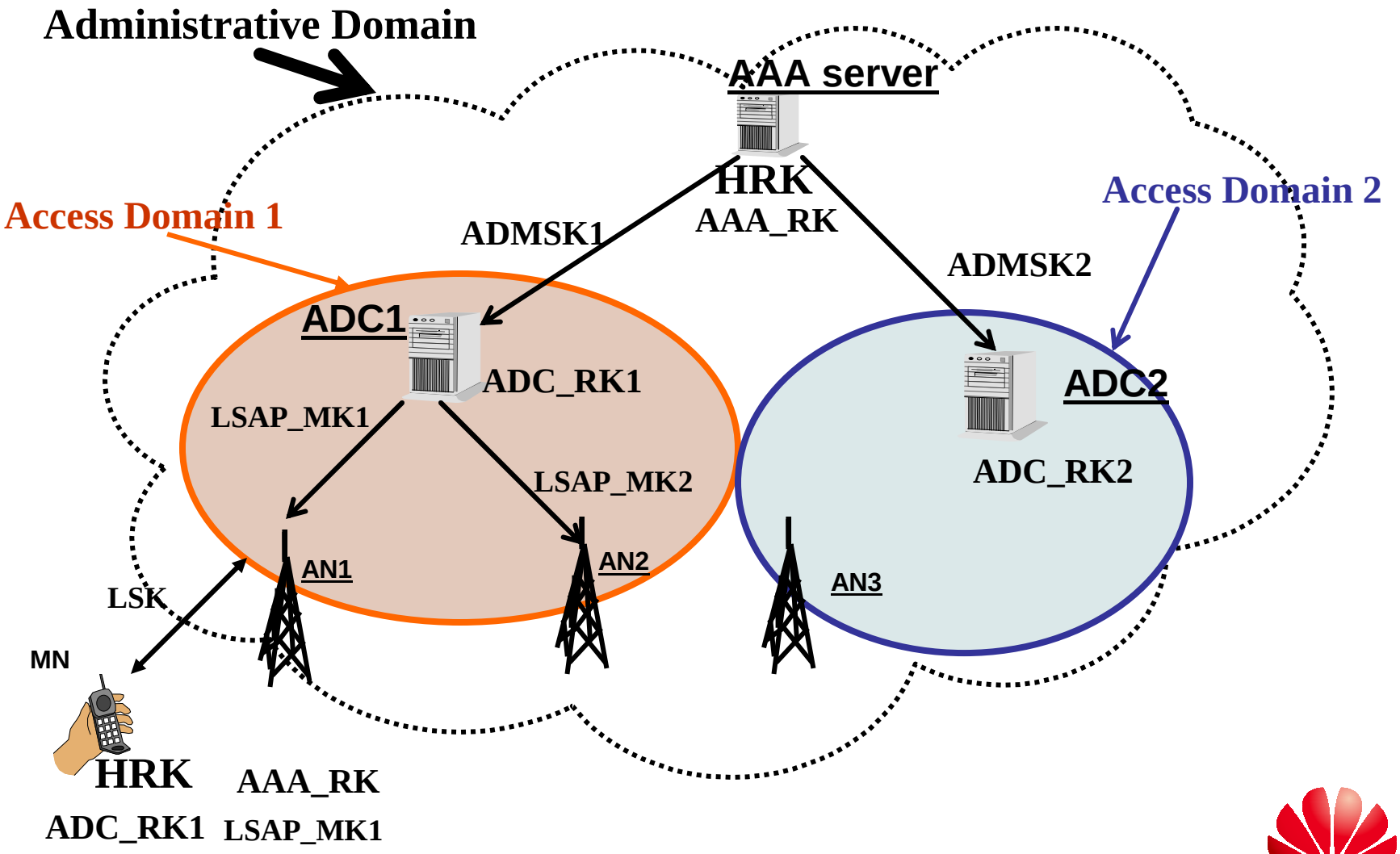
HUAWEI

Main Ideas

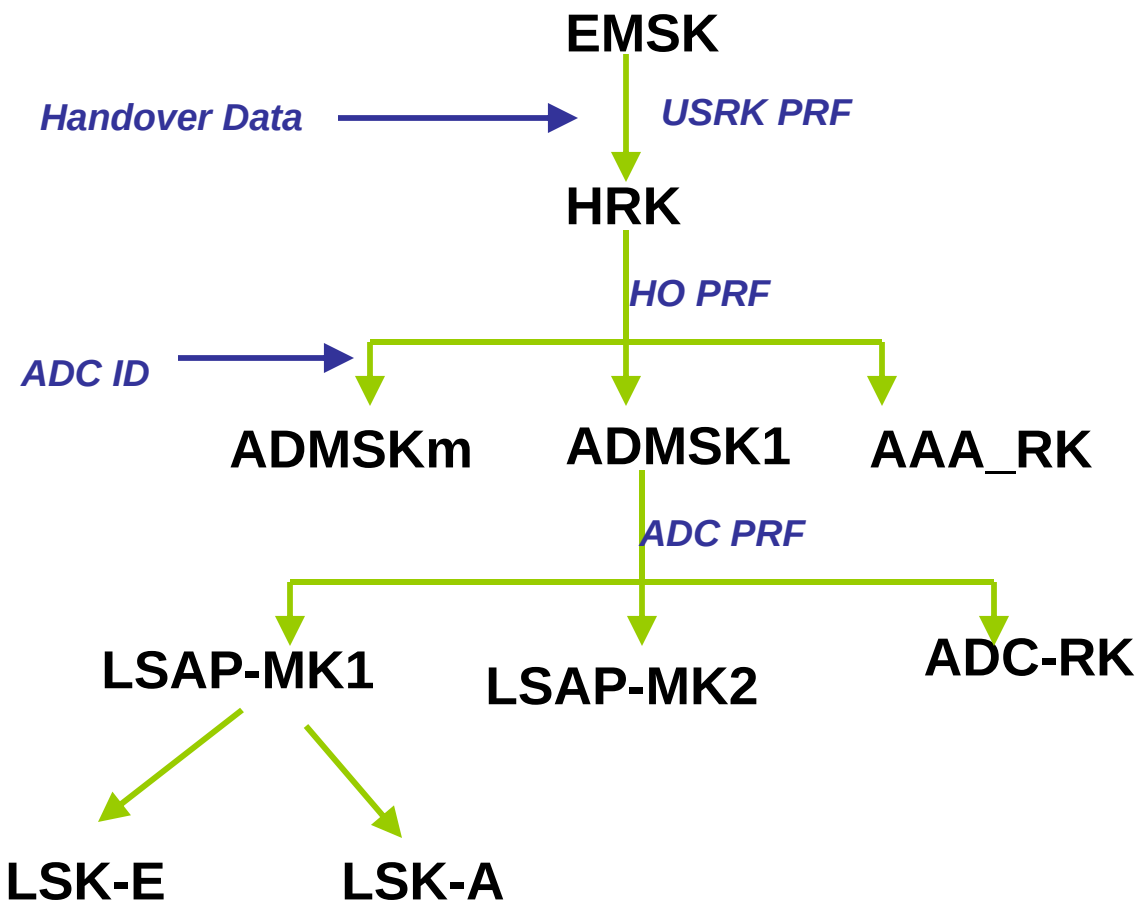
- Architecture allowing for access gateways
  - Handling many handovers without interaction with AAA.
- Key hierarchy for Authenticator (ADC) handovers and fast re-authentications to AAA
- Key hierarchy for handovers within Access domain
- Handover keying Signaling
- Channel binding for different levels of key hierarchy
- Signaling EAP method independent

HUAWEI

Assumed architecture and Keying hierarchy



Key generation

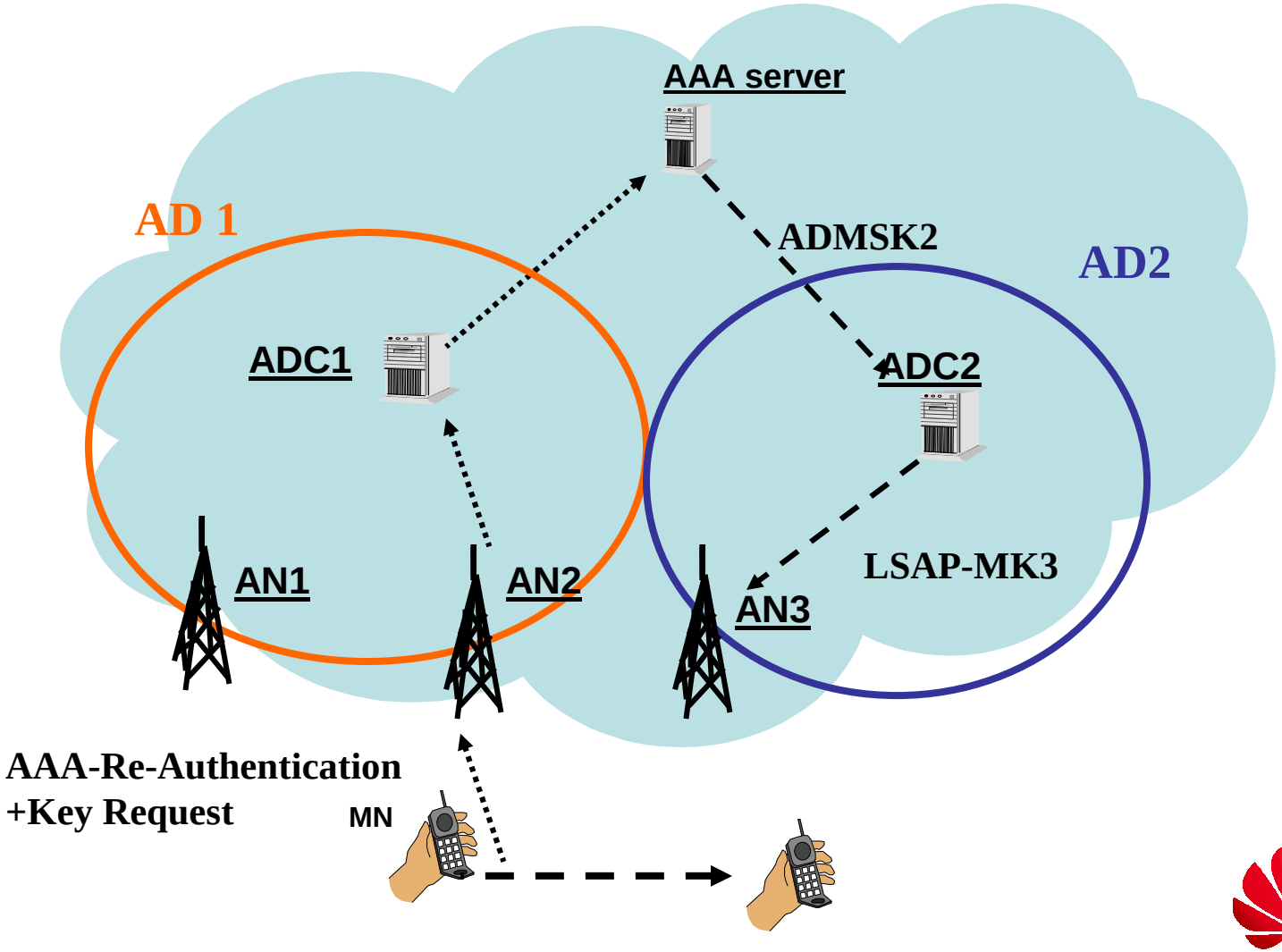


Key generation considerations

- HRK is derived from EMSK as USRK
  - EAP server holds EMSK and derives HRK
  - AAA server holds HRK
  - PRF based on USRK guidelines: default or negotiated
- AAA server is HRK Key Holder, HRK used for
  - AAA_RK: fast re-authentication/ADC handover authorization/ADMSK channel binding
  - Per-Authenticator/ADC keys (ADMSK)
  - PRF chosen for handover
- ADC is ADMSK Key holder, ADMSK used for
  - ADC_RK: fast re-auth to ADC/ AN handover authorization/ LSAP_MK channel binding
  - LSAP_MK: link SAP Master keys for ANs.

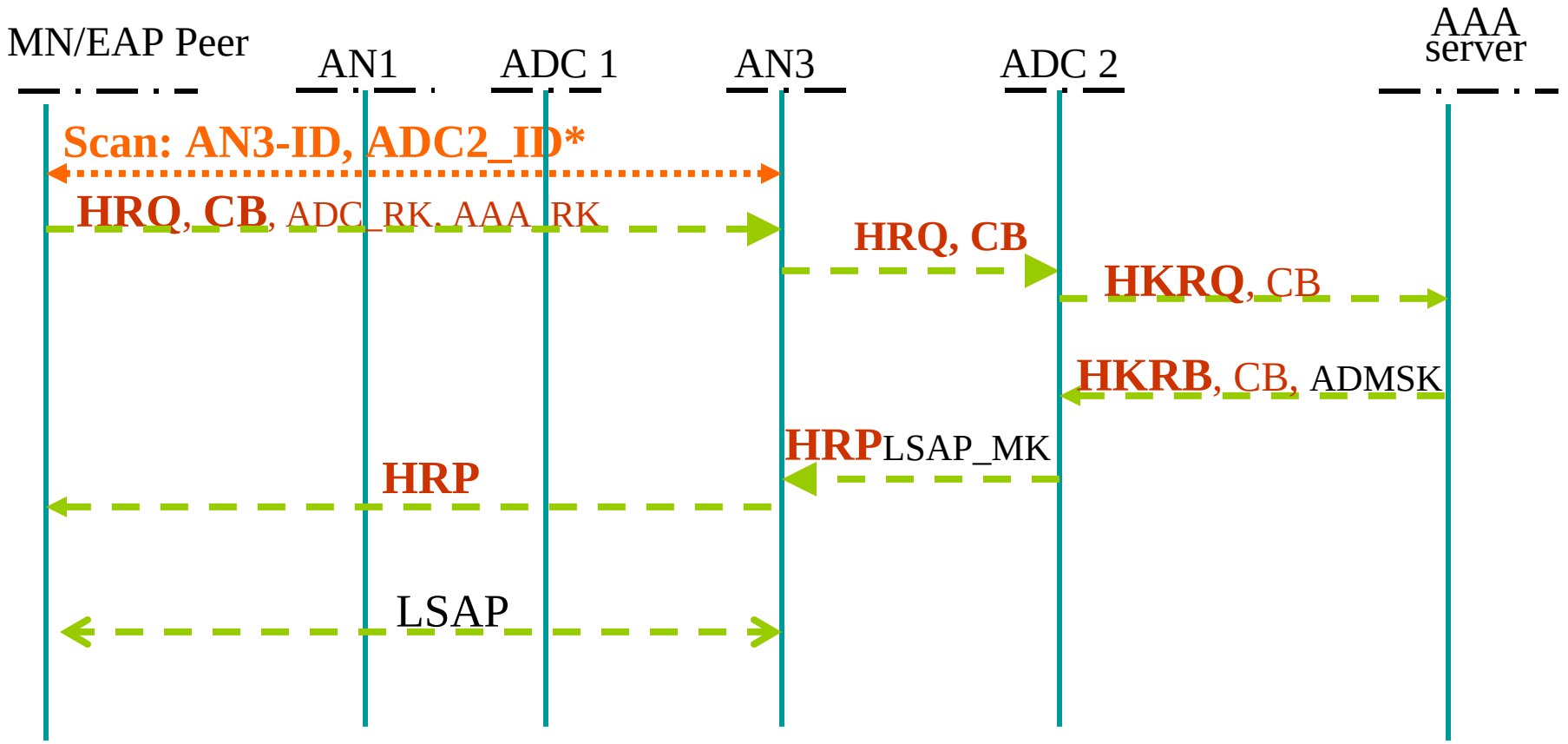
HUAWEI

Inter-ADC handover scenario

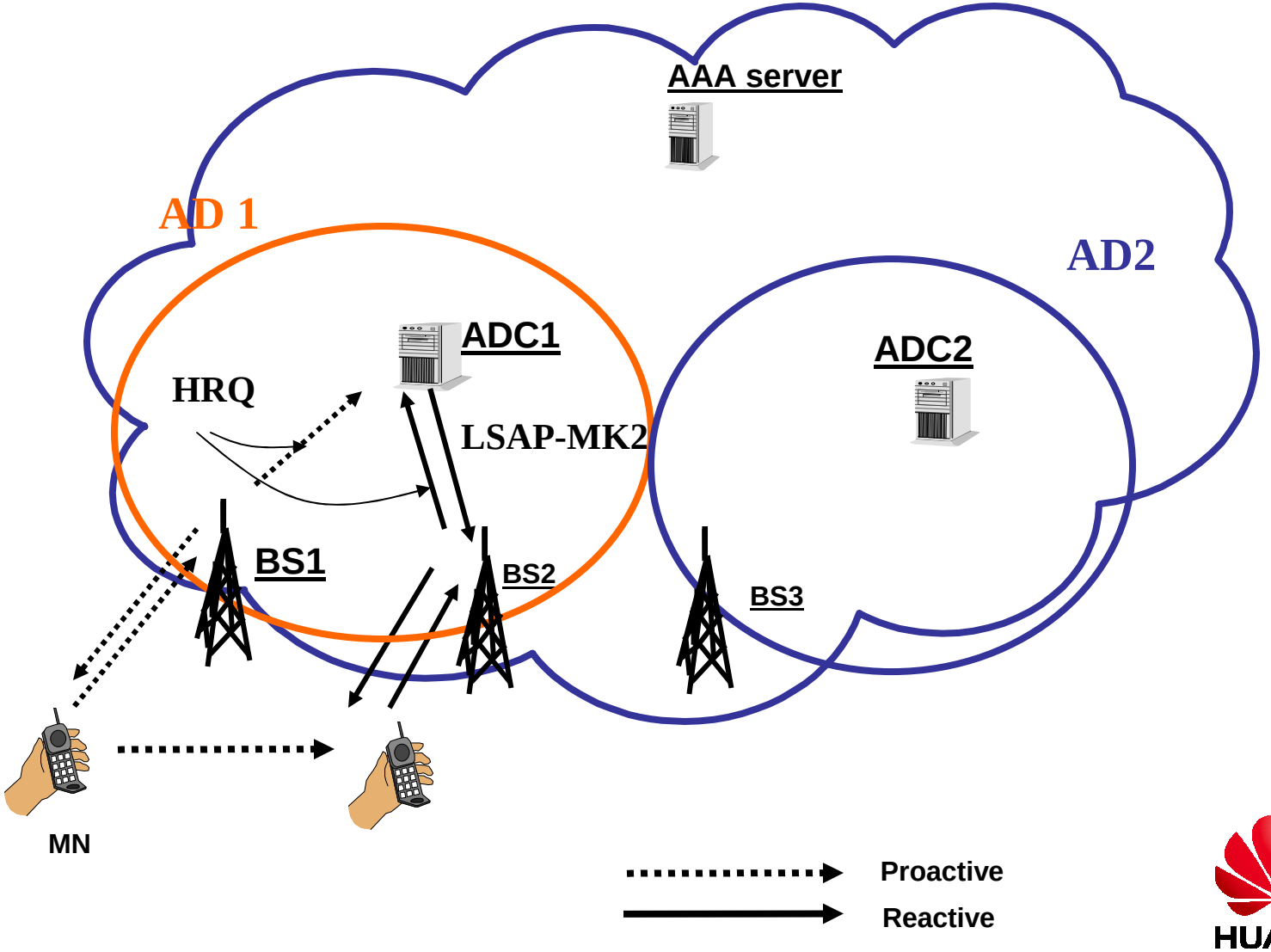


HUAWEI

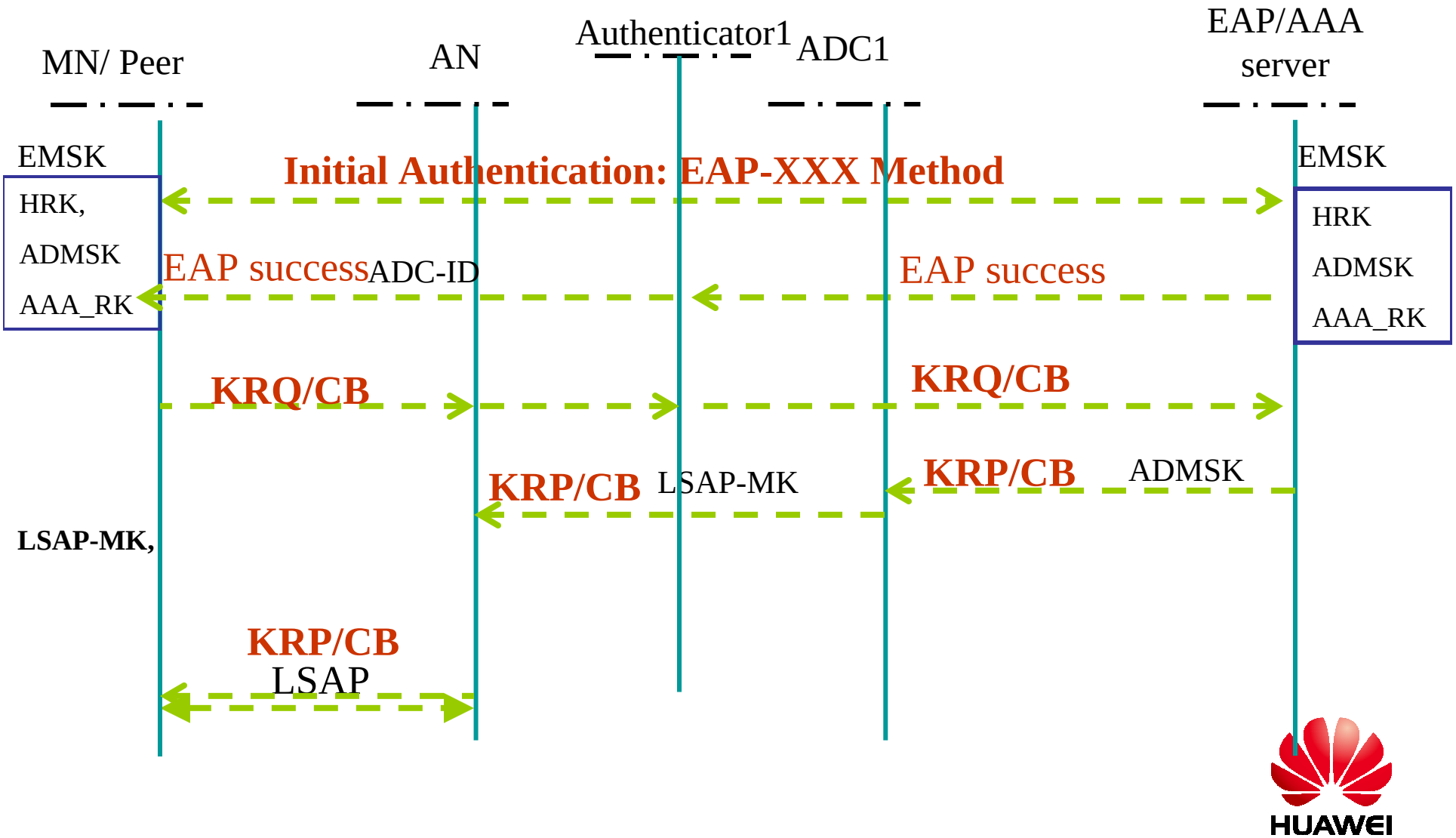
Inter-ADC Handover Keying/ reactive



Intra-ADC handover scenario



Suggestion 1: Initial entry/ EAP compatibility



Signaling alternatives

- Hokey messaging:
  - no change to EAP 3748
  - Diameter hokey application and all AVPs
- New EAP code:
  - Requires additions to EAP 3748
  - Diameter EAP application (DER/DEA), OK?
  - RADIUS EAP, OK
  - May impact lower layer encapsulation design.
- New EAP method:
  - Means sequencing EAP conversations.
  - Server based: requires trigger into the server to start Hokey-Reauth
  - May not require lower layer encapsulation
- EAP method encapsulation
  - Still server based
  - Crypto binding

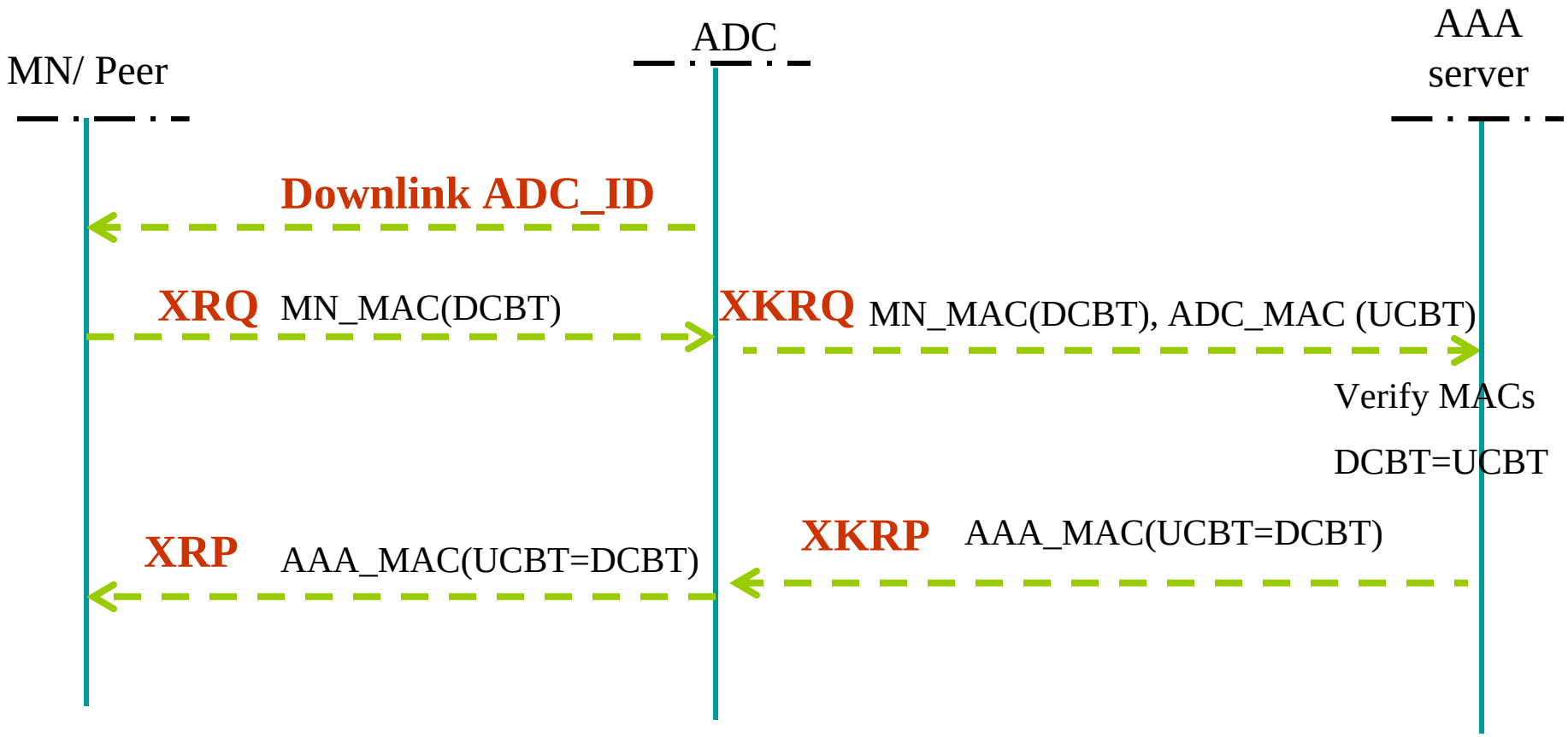
HUAWEI

Channel binding

- Channel binding Tuple (CBT)
  - (party 1 ID, party 2, other info)
  - Peer-ADC channel: (peer_ID, ADC_ID, other info)
- If lying ADC: Two CBT copies
  - Downlink: DCBT includes ADC_DID:
    - ADC to MN, reported and signed by MN
  - Uplink: UCBT includes ADC_UID:
    - ADC to AAA, reported and signed by MN
  - DCBT and UCBT must include matching ADC_IDs.
- Signature keys
  - MN: AAA_RK, both channel binding and re-authentication
  - ADC: ADC-AAA key

HUAWEI

Channel binding (No new messages) extensions and AVPs defined in draft



XRQ: HRQ or KRQ

XKRQ: HKRQ or KRQ

HUAWEI